(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 May 2001 (25.05.2001)

PCT

(10) International Publication Number
WO 01/37562 A1

(51) International Patent Classification[7]: H04N 5/913, 7/16

(21) International Application Number: PCT/EP00/11485

(22) International Filing Date:
17 November 2000 (17.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/444,490 19 November 1999 (19.11.1999) US

(71) Applicant: SCM MICROSYSTEMS GMBH [DE/DE]; Sperl-Ring 4 Hettenshausen, 85276 Pfaffenhofen (DE).

(72) Inventors: VANTALON, Luc; 1396 Cordilleras Avenue, Sunnyvale, CA 94087 (US). CHATAIGNIER, Arnaud; 31, allée de la Granette, F-13600 Ceyreste (FR). GENEVOIS, Christophe; 47, avenue de la Paix, F-13600 La Ciotat (FR).

(74) Agent: DEGWERT, Hartmut; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

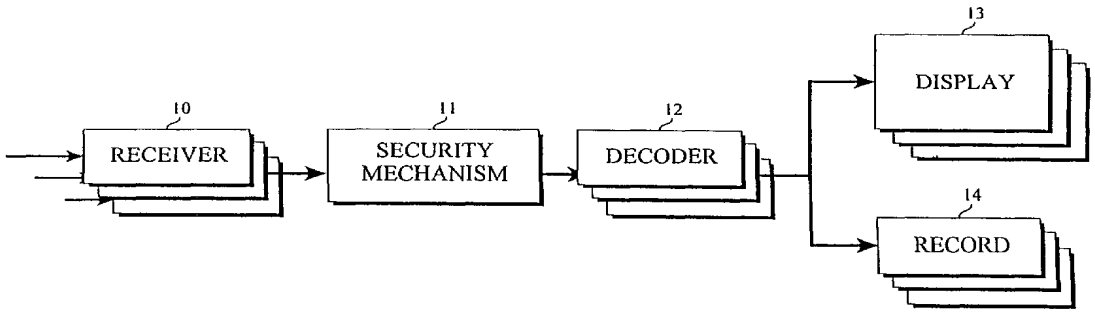
(81) Designated States *(national)*: JP, SG.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ADAPTIVE TRANS-SCRAMBLING MECHANISM FOR DIGITAL TELEVISION MULTIPLE DATA TRANSPORT SYSTEM



(57) Abstract: Conditional access methods and apparatus are provided for use with digital television receivers and other digital broadband receivers and permits multiple encryption formats. The methods and apparatus are capable of handling several different digital signal transmission protocols in an automatic and flexible manner. An input unit is provided for analyzing and tagging incoming data bytes so that further processing operations are less dependent on the transmission format being received. A cipher handling unit is provided for adapting in real time the scrambling and descrambling performances to match the format, encryption block size, and desired level of copy protection. A filtering mechanism is provided for filtering and handling multiple asynchronous data streams in a parallel manner.

WO 01/37562 A1

ADAPTIVE TRANS-SCRAMBLING MECHANISM FOR DIGITAL TELEVISION MULTIPLE DATA TRANSPORT SYSTEM

DESCRIPTION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to the following copending patent applications: U.S. Serial No. 09/444,488 , filed on Nov. 19, 1999 , entitled "Digital Television Conditional Access Methods and Apparatus with Multiple Data Transport Mechanism" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois; U.S. Serial No. 09/444,495, filed on Nov. 19, 1999 , entitled " Digital Television Methods and Apparatus" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois; and U.S. Serial No. 09/443,173 , filed on Nov. 19, 1999 , entitled "Signal Filtering Mechanism for a Multi-Purpose Digital Television Receiver" and invented by Luc Vantalon, Arnaud Chataignier, and Christophe Genevois. The foregoing cross-referenced patent applications are expressly incorporated in their entirety into this application by this reference thereto.

TECHNICAL FIELD

This invention relates to conditional access methods and apparatus for use with digital television systems and services. More particularly, the invention relates to multiple data streams used in the transfer of data in different encryption formats.

BACKGROUND OF THE INVENTION

Digital television is an emerging technology which is becoming increasingly popular with the public. One of the more interesting aspects is the introduction of so-called "high-definition television" (HDTV), the broadcasting of which was recently approved by the United States Federal Communications Commission. HDTV will provide television images of much higher quality and definition than is provided by preexisting "conventional definition" television systems. Another highly important

aspect of digital television is the providing of related services, such as video-on-demand programming, pay-per-view movies and sporting events, interactive video games, home shopping capabilities, high-speed Internet access and the like. The home television set is fast becoming the predominate information and services dispensing medium of the future.

As is known, television services are presently communicated by land-based radio-type broadcast transmissions, cable network transmissions and space satellite transmissions. In order to limit reception to paid subscribers, it is common practice for cable and satellite providers to scramble their transmissions and to require their customers to use a special set-top control box to unscramble the received signals. Such scrambling and set-top box techniques are also desired by providers of related services. The problem to date is that each provider has developed its own unique and proprietary set-top control box. Thus, to receive and use signals from multiple providers requires the use of multiple set-top control boxes. This is not the best situation and, in order to overcome the problem, the U. S. Federal Communications Commission is encouraging a so-called "open" set-top box approach for providing a universal set-top box capable of receiving and handling content from multiple providers. Unfortunately, this is not an easy thing to do since at the same time it has to provide the security control features needed to protect each service provider from loss of services to unauthorized users.

SUMMARY OF THE INVENTION

According to the present invention, real time adaptive descrambling and scrambling is performed on each received data byte according to the network encryption and transport mechanism, the set-top box decryption capabilities, and the position and the value of the current and previous data bytes within the same transport packet/cell unit.

In case of a received data byte that belongs to an unscrambled packet/cell or to a clear section (e.g. header, adaptation field) of a scrambled packet, the real time adaptive descrambling and re-scrambling mechanism just passes it through. In the case of a received data byte that belong to a scrambled section of a scrambled packet, its position within the packet determines the descrambler and re-scrambler mode of operation (e.g.,

without limitation, ECB, CBC and OFC feedback modes). A scrambled data byte, which is included in a section of eight contiguous scrambled data bytes, is processed by the real time adaptive descrambling and re-scrambling mechanism as a full block. When the scrambled data byte belongs to a section that includes less than eight contiguous data bytes, if its section is following a full block then it is processed as a termination block. If its section is following an unscrambled section, it is processed as a solitary block. When a scrambled data byte has been descrambled, if it belongs to a channel that requires some copy protection, as indicated to the real time adaptive scrambling mechanism by the conditional access application, it will be re-scrambled according to the same mode of operation as the one used for descrambling.

The present invention supports multiple cryptographic engines (DES, 3DES, DVB and MULTI II) that are called into operation by the real time adaptive descrambling and re-scrambling mechanism for each scrambled data byte. In the case of unencrypted data, a clear output is provided. In the case of encrypted data, a unit size of the received data unit is determined and a decrypting function is performed in accordance with the unit size. This provides decrypted data and according to the invention a determination is made of whether the decrypted data includes a copy protection indicia. If the decrypted data includes a copy protection indicia, an encryption function is performed in accordance with the unit size and the encrypted data is supplied as output.

The invention contemplates real time adaptive descrambling which is accomplished by selecting a desired descrambling format and selecting a session key. According to one particular aspect of the invention, a descrambling format is selected from a group which may include DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB.

According to another aspect of the invention, re-scrambling is accomplished in accordance with a detected copy protection status. The copy protection status is first determined to assess whether copy protection is desired, and if the copy protection status determination is negative, a clear packet cell byte is output. If the copy protection determination is affirmative, then a determination of block status is made, and the signal is scrambled according to the block status. If the block determination for a first

size is negative, a shorter block determination is made, and if the shorter block determination is affirmative, then the shorter block scrambling is undertaken.

According to a further aspect of the invention, a copy protect scrambler includes a scramble format register and multiple encoders. The scramble format register is configured to hold a plural-bit control signal and the encoders provide encoding of a TSclear signal from a descrambler in accordance with any one of a selected plurality of encryption formats. The encoders are configured to be individually selected by a plural-bit control signal which is loaded into a scramble format register.

According to one embodiment, the copy protect scrambler includes an enable signal decoder which is configured to activate a selected one of multiple output lines. The output lines are individually connected to different ones of the encoders.

In yet another aspect of the invention, a multiple scrambling method includes making a channel change, selecting a network descrambling mechanism, making a scrambling session key change, and loading a new session key. A qualified packet cell byte is received and a determination is made as to whether the received qualified packet cell is scrambled. If the received qualified packet cell is not scrambled, then a clear packet cell byte is output.

In one aspect of the invention, a multiple transport system is provided for enabling a conditional access module to handle any of a plurality of transport stream formats. The system includes a qualification mechanism, a tagging mechanism, a scramble format register and encoders for each encoding a Tsclear signal from a descrambler in accordance with any one of several encryption formats. The qualification mechanism processes received data bytes according to position and value within a packet and the tagging mechanism applies a multibit tag to each received data byte, containing information required for further processing of the byte. The scramble format register holds a plural-bit control signal and the encoders are individually selected by the control signal. In one particular embodiment, an enable signal decoder activates a selected one of several output line individually connected to different ones of the encoders and a scrambled data stream is provided at the output of the selected encoder.

The present invention provides an efficient and flexible security mechanism for use with a "universal" set-top control box. This security mechanism grants conditional access to the transmitted program material in a manner which provides a high degree of protection against unauthorized use of the material. This conditional access mechanism includes a multi-transport capability which performs descrambling and filtering operations on different transmission protocols by qualifying the different components of the transport layer using a unique coding technique.

The multiple transport apparatus of the present invention is capable of automatically handling several different data transport stream formats. It can, for example, handle MPEG, DSS and ATM type data transport streams. This is accomplished by qualifying each newly-received data byte according to its position and value within its packet. A plural-bit tag is assigned to each data byte, such tag having a value determined by the qualifying process. The qualified and tagged data byte provides all the information required for further processing of the data byte. The qualification mechanism is unique and is not dependent on the transport system used for carrying the received packet bytes. The qualification mechanism supports both broadcast and burst transmission modes and it provides all the information required for further processing.

In accordance with one aspect of the invention, a set top box receives multiple input data streams. These data streams take the form of transport streams, each of which may be in parallel or serial formats. The streams are multiplexed and then parsed so as to select a particular stream for a desired output. This permits a common set top box to receive data in different formats and yet selectively process the desired data.

The data from the multiplexer to be parsed is first buffered. The buffering is performed on a FIFO memory and provides the data to a parser. In the preferred embodiment, multiple FIFOs and parsers receive the buffered data. Since multiple parsed outputs are available, a selection of parsed transport streams is possible. This selection is performed through a selectionizing parser which receives individual transport streams from the parsers and selects outputs for the individual transport streams.

In one embodiment of the invention, two parallel transport streams and one serial transport stream are received. The data from the multiplexer to be parsed is first synchronized by providing multiple outputs to synchronizers which in turn provide corresponding outputs to respective FIFO memories. This permits simultaneous parsing of the multiple transport data streams so that the selectionizing parser is able to better manipulate the data.

By synchronizing the transport streams, it is possible to receive encrypted data on one stream and use information from another stream to decrypt the data. The synchronization permits the decryption information to be applied to the appropriate portion of the data.

According to a further aspect of the invention, new information is received in the form of a new packet or cell byte. The data is analyzed to determine if it is scrambled, and is either output as a clear packet or descrambled accordingly. In descrambling the packet, the packet is analyzed to determine if it is a full block, short block or a solitary block. Then full block, short block or solitary block descrambling is performed as appropriate.

The descrambled data is analyzed to determine if the data is copy protected and is either output as a clear packet or descrambled accordingly. In the case of copy protected data, the data is output with the cognizant form of scrambling; otherwise the output is provided as a clear packet.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring to the drawings:

FIG. 1 is a general block diagram of a digital television receiving system with a security mechanism for preventing unauthorized display of the transmitted images;

FIGS. 2A-2D show different ways of packaging the apparatus of FIG. 1;

FIG 2E is a block diagram of an adaptive trans-scrambling system according to one embodiment of the present invention;

FIG. 3 is a conceptual diagram for one embodiment of the present invention;

FIG. 4 shows in greater detail a representative form of internal construction for the set-top box and the conditional access module of FIG. 2B;

FIG. 5 is a detailed block diagram for the transport stream co-processor and the microprocessor unit of the conditional access module of FIG. 4;

FIG. 6 shows a representative form of construction for an out-of-band channel feature of the present invention;

FIG. 7 shows a representative form of construction for a microprocessor-to-microprocessor data channel feature of the present invention;

FIG. 8 shows a representative form of construction for a Smart Card channel feature of the present invention;

FIG. 9 shows representative form of construction for the transport stream (TS) input unit of FIG. 5;

FIG. 10 shows in more detail a representative form of construction for the cipher bank unit of FIG. 5;

FIG. 11 shows a general form of construction for the cipher processor of FIG. 10;

FIG. 12 shows the details of a representative form of construction for the conditional access descrambler of FIG. 11;

FIG. 13 shows the details of a representative form of construction for the copy protect scrambler of FIG. 11;

FIG. 14 shows a representative form of construction for the filter bank unit of FIG. 5;

FIG. 15 shows in greater detail the construction of one of the filter units of FIG. 14;

FIG. 16 is a plan view of one form of PCMCIA Smart Card reader that may be used with the present invention;

FIG. 16A is a left end view of the FIG. 16 card reader;

FIG. 16B is a right end view of the FIG. 16 card reader;

FIG. 16C is a side view showing one side of the card reader of FIG. 16;

FIG. 17 is a perspective view of another form of PCMCIA card reader that may be used with the present invention;

FIG. 18 shows a further form of card reader that may be used;

FIGS. 19, 20 and 21 show the packet formats for different types of data transport streams that may be handled by the present invention;

FIG. 22 is a flow chart used in explaining a multiple data transport feature of the present invention;

FIG. 23 is a detailed flow chart for a representative implementation of the method of FIG. 22;

Fig. 24 is a timing diagram for serial to parallel conversion according to the present invention, in which mistrt indicates the start of a new packet;

Fig. 25 is a timing diagram for serial to parallel conversion according to the present invention, in which sampling occurs on the rising edge of the mi_clock and the msb is the first bit of each byte;

Fig. 26 is a timing diagram for serial to parallel conversion according to the present invention, in which sampling occurs on the rising edge of the mi_clock and the lsb is the first bit of each byte;

Fig. 27 is a timing diagram for serial to parallel conversion according to the present invention, in which sampling occurs on the falling edge of the mi_clock and the msb is the first bit of each byte;

Fig. 28 is a timing diagram for serial to parallel conversion according to the present invention, in which sampling occurs on the falling edge of the mi_clock and the lsb is the first bit of each byte;

Fig. 29 is a timing diagram of stream synchronization according to the present invention, in which resynchronization on master_clock is permitted, and data is sampled on the falling edge of the ts_clock_in signal;

Fig. 30 is a timing diagram of stream synchronization according to the present invention, in which resynchronization on master_clock is permitted, and data is sampled on the rising edge of the ts_clock_in signal;

Fig. 31 is a diagram of stream FIFO architecture according to the present invention;

Fig. 32 is a state diagram of FIFO operation during which data is written into the FIFO according to the present invention;

Fig. 32A is a state diagram of FIFO operation during which data is read out of the FIFO;

Fig. 33 is a diagram of the architecture of a transport stream parser according to one embodiment of the present invention;

Fig. 34 is a diagram of the architecture of a DVB stream parser according to one embodiment of the present invention, with Fig. 34A being a block diagram of the parser system, and with Fig. 34B being a diagram of data inputs and outputs of a DVB parser, according to the present invention;

Fig. 35 is a diagram of the format of a DVB packet header according to one embodiment of the present invention;

Fig. 36 is a diagram of the architecture of a DSS stream parser according to one embodiment of the present invention;

Fig. 37 is a diagram of the architecture of DSS stream parsing operation according to one embodiment of the present invention, in which the packet is not scrambled;

Fig. 38 is a state diagram of DSS stream parsing operation according to the present invention;

Fig. 39 is a diagram of the architecture of an ATM stream parser according to one embodiment of the present invention;

Fig. 40 is a state diagram of ATM stream parsing operation according to the present invention;

Fig. 41 is a timing diagram of output stream interfacing operation according to the present invention;

Fig. 42 is a flow chart of a scrambling operation set up according to one embodiment of the present invention;

Fig. 43 is a flow chart of a descrambling operation set up according to one embodiment of the present invention; and

Fig. 44 is an overall flow chart of a trans-scrambling operation according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS

Referring to FIG. 1, there is shown a general block diagram of a digital broadband receiving system having one or more receivers 10 connected to one or more broadband signal transmission networks. Typical signal transmission networks include land-based radio-frequency type broadcast networks, cable networks, space satellite signal transmission networks, broadband telephone networks, etc. The analog information signals intended for transmission (for example: video signals, audio signals, or data signals) are converted to specific digital transport stream formats for transmission purposes. Typical transport stream formats are the MPEG format, the DSS format and the ATM format. The MPEG format is the data transmission format developed by the Motion Picture Expert Group. A preferred form of MPEG is MPEG-2, which is defined in ISO/IEC Standard 13818. The acronym "DSS" stands for Digital Satellite Systems and refers to a format developed for use in transmitting digital signals used by some satellite operators. The acronym "ATM" stands for Asynchronous Transfer Mode. It is a digital signal protocol for efficient transport of both fixed rate and burst information in broadband digital networks. The ATM digital stream consists of fixed length packets called "cells."

Each receiver 10 demodulates its received signal and supplies the demodulated signal to a security mechanism 11. Security mechanism 11 selects one or more of the received signal transport streams and removes the network distribution security layers therefrom, provided the end user is entitled to receive the signals. Network security mechanism 11 also applies content protection to any of the signal streams that require it. The resulting signals are supplied to decoders 12 which select one or more of the signal streams and decodes each selected stream to recreate the desired video, audio and data signals which are, in turn, supplied to one or more display units 13 and one or more recording units 14. Typical display units include television sets and television and computer monitors. Typical recording units include VCR-type video recorders and various types of computer memory units. Security mechanism 11 examines the received signal or signals and determines their types and controls their descrambling. Security mechanism 11 allows access to an unscrambled version of the received signal, provided the required conditions are met.

In addition to regular digital television programming, the receiving system of FIG. 1 also receives and handles various related communications services. Examples of related services are video-on-demand programming, pay-per-view movies and sporting events, interactive video games, home shopping services, high-speed Internet access, and the like. As will be seen, the data signals and control signals for these related services are supplied by way of a so-called "out-of-band" channel.

FIGS. 2A-2D show different ways of packaging the apparatus of FIG. 1. In particular, FIG. 2A shows the case where the receivers 10, security mechanism 11 and decoders 12 are located within a network specific set-top box 15. In one case, the security mechanism 11 is imbedded within or permanently mounted within the set-top box 15. In a typical use, the set-top box 15 sits on top of the display unit 13.

FIG. 2B shows an open-type set-top box 16 with a renewable and removable add-on security mechanism represented by a conditional access module (CAM) 17. Conditional access module 17 performs the security functions provided by the security mechanism 11 of FIG. 2A. Control access module 17 is a removable plug-in type element which is adapted to be plugged into a cooperating receptacle or socket in the host set-top box 16. As in FIG. 2A, set-top box 16 is designed to sit on top of the display unit 13.

FIG. 2C shows the case where the set-top box functions are located inside the cabinet 18 of a television receiver, that is, the cabinet which houses the display unit or picture tube 13. The conditional access module 17 is adapted to plug into a cooperative receptacle which is accessible from the outside of the cabinet 18. FIG. 2C represents an integrated television set with a renewable, add-on security mechanism represented by the conditional access module 17.

FIG. 2D represents the case where the primary units are located in separate component-type cabinets or boxes 19a-19d. The conditional access module 17 may be removably plugged into the receiver box 19a or the decoder box 19b or may, instead, be part of a small connector unit which is connected between boxes 19a and 19b. The configuration of FIG. 2D would be particularly useful in a component-type entertainment center intended for home use.

FIG 2E is a block diagram of an adaptive trans-scrambling system 7 according to one embodiment of the present invention. In particular, the adaptive trans-scrambling system 7 includes a transmitter 8 having an encryption system 9 for applying a selected one or more modes of encryption to respective one or more information channels which provide a packet stream or streams to a receiver 10. The receiver 10 includes a tuner system 10A for selecting one of the channels and its packet stream at a time. The user can adjust the tuner to select any of a number of channels. The adaptive trans-scrambling system further includes a conditional access module 17 which is connectable to a selected host by means of a PCMCIA connector 17A or the like. The host system may be a set-top box including a receiver 10 and a deconder 33 according to one embodiment. According to one embodiment of the present invention, the conditional access module 17 includes a decryption system 17B and a copy protect scrambler 17C. The host system may further include a decoder 33 which in turn includes a copy protect descrambler 33A. The decoder 33 is connected to a display 13 to enable user viewing. According to one embodiment, the conditional access module 17 includes a decryption loop which operates in connection with the decryption system 17B, to enable decryption deconvolutions which involve more than one loop through the decryption system 17 to facilitate decryption. In operation, within a single chip which comprises the conditional access module, one scrambling or encryption system is substituted for another. Accordingly, the conditional access system 17 acts as a bridge between two different encryption systems. One system is a local, perhaps set top specific copy protect encryption system which has its own rapidly changing key system. The conditional access module 17 further operates to handle channel decryption modes of many kinds with changeable decryption session keys.

Referring to FIG. 3, there is shown a conceptual diagram for one embodiment of the present invention. As there seen, the receiving apparatus includes an in-band channel 20 and an out-of-band channel 21, which are adapted to receive incoming signals from a remote broadcasting station. The in-band channel 20 handles the primary user signals, such as the digital television signals. The out-of-band channel 21, on the other hand, handles the digital signals for the related services, such as video-on-demand commands, security data, e-commerce transactions, etc. Both of channels 20

and 21 communicate with various application programs 22 by way of a filter bank 23 which detects various defined digital patterns within the received signals and reacts thereto for establishing connections with the appropriate ones of applications 22.

The apparatus of FIG. 3 also includes a smart card channel 24 for providing communications between a smart card SC and the applications programs 22. A data channel 25 provides communications between a CPU (Central Processing Unit) located in the host unit, for example, set-top box (STB) 16, and the application programs 22. An extended channel 26 is provided to transfer network data over the out-of-band channel from the network to the host CPU or vice versa.

Referring to FIG. 4 there is shown in greater detail a representative form of internal instruction for the host unit or set-top box 16 and the conditional access module 17 of FIG. 2B. As seen in FIG. 4, a signal connector 29 connects the set-top box 16 to the communications network supplying the signals. This signal path 29 runs to an in-band receiver 30 and an out-of-band receiver 31. The communications network is a multi-channel system and the channel conveying the primary video and audio signals is labeled as the "in-band" channel and the channel which carries the signals for the related services is called the "out-of-band" channel. The set-top box 16 further includes an out-of-band transmitter 32 for transmitting signals back to the digital data provider located at the network broadcasting center.

The digital signals appearing at the outputs of receivers 30 and 31 are supplied to the conditional access module 17. The primary video and audio signals are supplied back to a decoder 33 in the set-top box 16 and from there to the digital TV display 13. The set-top box 16 includes a microprocessor unit 34 which, among other things, provides control signals to the decoder 33. A memory unit 36 is coupled to the microprocessor unit 34 and, among other things, provides storage for various control routines and application program functions utilized by the microprocessor unit 34. Microprocessor unit 34 and memory 36 provide a CPU function for the set-top box 16.

The conditional access module (CAM) 17 of FIG. 4 includes a transport stream (TS) co-processor 40 which receives the output digital signals from the in-band receiver 30 and the out-of-band receiver 31, the latter being supplied by way of an out-of-band decoder 41. Transport stream co-processor 40 also supplies the digital video and digital

audio signals which are intended for the TV display 13 to the decoder 33. Conditional access module 17 further includes a microprocessor unit 42 and an associated memory unit 43. These units 42 and 43 provide a CPU function for the conditional access module 17. The primary portion of the application programs 22 are stored in the memory 43. A data channel 44 provides a direct communications link between the CAM microprocessor unit 42 and the host microprocessor unit 34. The CAM microprocessor unit 42 can also send digital messages and information back to the network broadcasting center. This is done by way of an out-of-band encoder 45 and the out-of-band transmitter 32 in the host set-top box 16. A removable smart card 28 is adapted to be connected to the microprocessor unit 42 for supplying control information thereto.

An extended channel is provided for enabling the network broadcasting center to communicate with the host microprocessor unit 34 and vice-versa. The incoming branch of this extended channel includes a signal path 47 coupled to the out-of-band receiver 31 and extending to the out-of-band decoder 41. This incoming branch includes the decoder 41, transport stream co-processor 40, microprocessor 42 and a further signal path 49 which runs from the microprocessor 42 to the host microprocessor 34. The outgoing branch of this extended channel is provided by a signal path 50 which runs from the host microprocessor 34 directly to the out-of-band encoder 45.

Referring to FIG. 5, there is shown a detailed block diagram for the transport stream (TS) co-processor 40 and the microprocessor unit 42 of the conditional access module (CAM) 17 of FIG. 4. As seen in FIG. 5, the transport stream (TS) co-processor 40 includes a transport stream (TS) input unit 52 which receives parallel- type digital input signals TSin1 and TSin2 from the in-band receiver 30 and the out-of-band receiver 31, respectively. A serial-type digital signal TSin3 is received from the out-of-band receiver 31. The output signals from the input unit 52 are supplied to a cipher bank 54 for further processing. Cipher bank 54 produces two parallel type output streams which are connected to the inputs of a TS output unit 55 and a filter bank 56. By multiplexer selection within the cipher bank 54, one of the two input streams to the cipher bank 54 is processed by an internal cipher processor, while the other input stream

is simply bypassed to the TS output unit 55 and the filter bank 56. The TSout signal from TS output unit 55 is supplied to the decoder 33 in the set-top box 16.

The transport stream input unit 52 includes a multiple data transport mechanism capable of receiving a plurality of different transport stream formats. In particular, it includes a qualifying mechanism for receiving and qualifying incoming data bytes according to their positions and values in their plural-byte data packets. TS input unit 52 further includes a tagging mechanism for assigning a plural-bit tag to each data byte, such tag having a unique value determined by the results of the qualifying process. The tag bits are used to facilitate the further processing of the data bytes.

The microprocessor unit 42 includes an ARM7 microprocessor 60 which is connected to a 32-bit ARM system bus ASB which typically operates in a high speed transfer mode. Also connected to the ASB bus are a memory interface unit 61, an address decoder unit 62, an arbiter unit 63, and a read only memory (ROM) unit 64. Memory interface 61 is connected to the external memory 43 associated with the microprocessor unit 42.

The microprocessor 60 communicates with the transport stream coprocessor 40 and various other units by means of a VLSI peripheral bus VPB. This VPB bus is connected to the microprocessor 60 by way of a bus-to-bus bridge unit 65 and the high-speed ASB bus. The ASB bus is used for fast transfers and the VPB bus is used for communications with a lower priority. As the filter bank 56 of co-processor 40 needs a direct and fast access to the external memory 43 for its output data, it is also connected to the ASB bus. As a consequence, there are three masters on the ABS bus, namely, the microprocessor 60 and the two channels of the filter bank 56. The arbitration between these masters is managed by the arbiter unit 63. By way of comparison, the VPB bus has only a single master, namely, the microprocessor 60.

The address decoder 62 decodes the address bits on the ASB bus to select the right target for the data on the ASB bus. Typical targets are the memory interface 61, ROM 64 and the various peripherals and other units connected to the ASB bus. An interrupt controller 66 provides the interrupt function for the microprocessor 60, while a timer 67 provides various timing functions. Each of the units in the transport stream co-processor 40 is coupled to the lower priority VPB bus for control and status purposes.

Also coupled to the VPB bus are an extended channel unit 68, a data channel unit 69 and a PCMCIA interface 70. A peripheral interface unit 71 provides an interface between the VPB bus and one or more peripheral devices. For example, a smart card interface connector structure 72 is provided for making connection with a removable smart card 28 shown in FIG. 4. A serial interface 73 may be provided for connecting to a serial type peripheral device PD.

FIG. 6 shows a representative form of construction for an out-of-band channel feature of the present invention. This out-of-band channel feature includes an out-of-band channel decoder 41 which receives the out-of-band signal OBin from the out-of-band receiver 31 shown in FIG. 4. The output of decoder 41 is supplied by way of the transport stream co-processor 40 for further filtering operations. The outgoing or transmitter portion of the out-of-band channel includes ATM encoder 48, transmit buffer 46 and a channel encoder 45 which supplies the out-of-band output signal OBout to the out-of-band transmitter 32 shown in FIG. 4. The ATM encoder 48 receives its input signal from the VPB peripheral bus associated with the microprocessor unit 42. The data to be transmitted is supplied by either the application programs located in the microprocessor unit 42 or the data received from the set-top box 16 by way of the extended channel path 50. This data is segmented into ATM cells by the ATM encoder 48. These cells are temporarily stored in a buffer 46. When the network grants some transmission slots to the conditional access module 17, the transmit buffer 46 is emptied by channel encoder 45 and is transmitted by way of out-of-band transmitter 32 to the network broadcast center.

FIG. 7 shows a microprocessor-to-microprocessor data channel feature of the present invention. This feature enables the CAM microprocessor unit 42 to communicate directly with the host microprocessor unit 34 and vice-versa. Microprocessor unit 42 sends data to the microprocessor unit 34 by way of data channel 44a. The host unit 34 sends data to the CAM microprocessor 42 by way of data channel 44b.

FIG. 8 shows the details of the smart card interface 72 of FIG. 5. The smart card 28 is adapted to be inserted into a smart card reader 86 and the data received from the smart card 28 is supplied by way of an input buffer 87 to the peripheral bus VPB

associated with the microprocessor unit 42. Data from the microprocessor unit 42 is supplied by way of the VPB bus, output buffer 88 and the smart card reader 86 to the smart card 28. In a representative embodiment, smart card reader 86 is a PCMCIA card reader. The acronym PCMCIA stands for Personal Computer Memory Card International Association. This is a non-profit trade association founded in 1989 to define a standard memory card interface. The smart card reader 86 complies with this interface standard.

Referring now to FIG. 9 there is shown in greater detail a representative form of construction for the transport stream input unit 52 of FIG. 5. The TSin1 and TSin2 signals are supplied to input registers 130 and 131. The serial input signal TSin3 is supplied to a serial-to-parallel converter 132 which converts same from serial form to parallel form. The parallel output of converter 132 is supplied to a further input register 133. The outputs of registers 130, 131, and 133 are connected to a three-to-two multiplexer 134. This multiplexer 134 selects two out of the three inputs and supplies one of the selected inputs to a TS1 FIFO unit 135 and the other of the selected inputs to a TS2 counter unit 136. FIFO 135 provides the input for a TS1 parser 137, while the counter 136 provides the input for a TS2 parser 138. Parsers 137 and 138 analyze their respective signal streams on a byte-by-byte basis and assign a plural-bit tag to each data byte. More particularly, each of parsers 137 and 138 includes a qualifying mechanism for receiving and qualifying incoming data bytes according to their positions and values in their plural-byte data packets. In a representative embodiment, a 5-bit tag is generated for and attached to each data byte. The value of this 5-bit tag is determined by the qualifying process performed by the qualifying mechanism. Parsers 137 and 138 are, in turn, connected to a selection parser 139 which determines the particular output path, TSa or TSb, to which each data stream is connected.

Referring to FIG. 10, there is shown in more detail a representative form of construction for the cipher bank 54 of FIG. 5. Cipher bank 54 receives the two signal streams TSa and TSb from the TS input unit 52 of FIG. 9. The two output buses 74 and 75 from cipher bank 54 are connected to the TS output unit 55 and the filter bank 56. Thus, the cipher bank 54 has two input streams and two output streams. By selection via multiplexers 76, 77, and 78, one of the input streams is processed by a cipher

processor 79, while the other input stream is simply bypassed to the output of its corresponding one of multiplexers 77 and 78. Multiplexers 76, 77 and 78 are controlled by selection signals S1, S2 and S3, respectively, obtained by way of the VPB bus.

For a first set of multiplexer settings, the TSa data stream is transferred by way of multiplexer 76 to the cipher processor 79 and the output of cipher processor 79 is transferred by way of multiplexer 77 to the TSout1 bus 74 of the cipher bank 54. For this same case, the second input data stream TSb, is supplied by way of multiplexer 78 to the TSout2 bus 75. For the second set of multiplexer settings, the situation is reversed. The TSb data stream is supplied by way of multiplexer 76 to the cipher processor 79 and the resulting processed signal is supplied by way of multiplexer 78 to the TSout2 bus 75. In this second case, the TSa input data stream is supplied by way of multiplexer 77 to the TSout1 bus 74. Cipher processor 79 outputs both a protected data stream TSp and a clear data stream TSc. Multiplexers 77 and 78 select one or the other, but not both of these data streams.

Referring to FIG. 11, there is shown the primary elements of the cipher processor 79 of FIG. 10. As seen in FIG. 11, cipher processor 79 includes a conditional access descrambler 80 and a copy protection scrambler 81. Descrambler 80 descrambles a scrambled incoming digital signal to produce a clear copy output signal TSclear. Descrambler 80 is capable of descrambling the following encryption formats: the DVB super scrambling format used in Europe, the DES and 3DES data encryption standard formats which are used in the United States, and the MULTI2 format which is used in Japan. The copy protect scrambler 81 is used to rescramble the clear copy signal at the output of descrambler 80 to preclude the data content from being stolen at the output of the conditional access module 17. Scrambler 81 uses the DES data encryption standard scrambling method.

FIG. 12 shows the details of a representative form of construction for the conditional access descrambler 80 of FIG. 11. The descrambler 80 of FIG. 12 includes an input data register 140 for receiving the TSin data stream from the multiplexer 76 of FIG. 10. Descrambler 80 also includes a set of eight decoders 141-148 for descrambling any one of the following encryption formats: DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB. Other

encryption formats can be accommodated by providing appropriate additional decoders. The foregoing acronyms have the following meanings:

ACRONYM	DESCRIPTION
DVB	Digital Video Broadcasting (Europe)
DES	Data Encryption Standard (U.S.)
ECB	Electronic Code Book
CBC	Chain Block Cipher
OFB	Output Feedback Block

The ECB, CBC and OFB formats are known variations of the DES and 3DES formats.

A descramble format register 150 and an associated decoder 151 determine which one of the primary decoders 141-148 is activated to process the incoming data stream. Descramble format register 150 is loaded by way of the VPB bus with a plural-bit control signal which designates the decoder to be used. This control signal is decoded by the enable signal decoder 151 to activate one and only one of its output lines. Thus, only a selected one of the decoders 141-148 is activated or used for any given data transport stream.

It is also necessary to load a session key register 152 with a descrambling session key which tells the selected one of decoders 141-148 how to descramble the incoming data stream. This descrambling key is loaded into register 152 by way of the VPB bus. Register 152, in turn, supplies the descrambling key to each of the decoders 141-148 and it is used by the decoder which is selected by the control signal in the descramble format register 150. The descrambled data stream appearing at the output of the selected one of decoders 141-148 is supplied to an output data register 153 to provide a clear or unscrambled output signal TSclear or TSc.

Referring now to FIG. 13, there is shown the details of a representative form of construction for the copy protect scrambler 81 of FIG. 11. For the embodiment shown in FIG. 13, the descrambler 81 includes a set of three encoders 155, 156 and 157 for encoding the TSclear signal from descrambler 80 in accordance with any one of the following three encryption formats: DES-ECB, DES-CBC and DES-OFB. Other scrambling formats may be used if desired. Selection of a desired one of the encoders 155-157 is accomplished by means of a plural-bit 7 control signal which is loaded into a

scramble format register 158. This control signal controls an enable signal decoder 159 to activate a select one of its output lines, which output lines individually run to different ones of the encoders 155-157. The scrambled data stream appearing at the output of the selected encoder is supplied to an output data register 160 to provide the copy protected output signal TSprotected or TSp. The actual scrambling process which is followed in the selected encoder is controlled by a plural-bit scrambling session key which is loaded into a session key register 161. This scrambling session key is obtained from the microprocessor unit 42 by way of the VPB bus.

Referring now to FIG. 14, there is shown a representative form of construction for the filter bank 56 of FIG. 5. This filter bank 56 examines incoming data streams to determine the type of data packets being received. When a desired packet is identified, its data payload is then stored in the proper location in memory 43 which is assigned to its particular packet type. In this way, the incoming data may be filtered or sorted according to the application or use for which it is intended. More particularly, the filter bank 56 has two inputs FLTin1 and FLTin2 which may convey different transport stream formats. For example, the first input FLTin1 can be connected to the in-band channel output from in-band receiver 30 and its data stream is assumed to use the MPEG packet format. The second input FLTin2 can receive the data stream from the out-of-band receiver 31 and the data signals of the this out-of-band channel are assumed to be of the asynchronous transfer mode (ATM) cell format.

The filter bank 56 includes four filter units 90-93 which can be independently set up to process different data streams. This architecture allows a flexible adjustment of the filtering resource depending on the type of application. For example, if the conditional access module is set up to support ATSC-type advanced television services (for example, high-definition television), the four filter units 90-93 are tuned to the in-band channel. For an open cable type of operation, on the other hand, up to three of the filter units can be set to process the out-of-band channel for collecting IP and proprietary messages, while the fourth filter unit must stay tuned to the in-band channel for processing in-band command signals. The outputs of filter units 90-93 are selectively connected to the microprocessor ASB bus by a multiplexer 94 which is controlled by switching signal S4.

FIG. 15 shows in greater detail a representative form of construction for one of the filter units 90-93 of FIG. 11. Each of the filter units 90-93 is of this same construction. The filter unit of FIG. 12 is tuned to one of the two inputs FLTin1 and FLTin2 by a multiplexer 95 which is set to select one of the two inputs by a selector signal S5. The selected input data stream is supplied to a Type Filter 96 which prefilters the data bytes according to the plural-bit tags attached to them in the TS input unit 52 of FIG. 9. The filtered bytes are then stored in an array of filter cells 97a-97h. Pre-recorded signal pattern which it is desired to detect are stored in a pattern memory 98 and are supplied to filter cells 97a-97h. When a pattern match occurs, the corresponding filter cell loads a shift register 99. Complete messages are extracted from shift register 99 for storage in the memory unit 43 associated with the CAM microprocessor unit 42.

FIG. 16 is a plan view of one form of PCMCIA smart card reader that may be used with the present invention. FIG. 16A is a left-end view, FIG. 16B is a right-end view and FIG. 16C is a side view of the card reader shown in FIG. 16. The acronym PCMCIA stands for Personal Computer Memory Card International Association. This is a non-profit trade association formed in 1989 to define a standard memory card interface. The smart card reader of FIG. 16 includes a metallic casing 100 which is adapted to receive a plastic memory card or smart card of approximately the size of a plastic credit card. The casing 100 conforms to ISO Standard 7816. In use, the smart card is inserted into the casing 100 and the casing 100 is, in turn, inserted into an appropriate connector receptacle in the set-top-box 16.

FIG. 17 is a perspective view of another form of PCMCIA card reader that may be used with the present invention. The reader casing 101 of FIG. 17 has a shorter extension, hence, a shorter overall length. FIG. 18 shows a further form of card reader that may be used. The reader casing 102 of FIG. 18 is a so-called dual reader casing and is adapted to receive two different smart cards.

FIGS. 19, 20 and 21 show the packet formats for different types of data transport streams that may be handled by the present invention. FIG. 19 shows the format for an MPEG data stream packet. FIG. 20 shows the format for a DSS data stream packet and FIG. 21 shows the format for an ATM data stream cell. The MPEG

format is the data transmission format developed by the Motion Picture Expert Group. The preferred form of MPEG is MPEG-2 which is defined in ISO/IEC Standard 13818. The acronym "DSS" stands for Digital Satellite Systems and refers to a format developed for use in transmitting digital signals by some satellite operators. The acronym "ATM" stands for Asynchronous Transfer Mode. It is a digital signal protocol for efficient transport of both constant rate and burst information in broadband digital networks. The ATM digital stream consists of fixed-length packets called "cells". Each cell contains 53 8-bit bytes and is comprised of a 5-byte header and a 48-byte information payload. The digital television signal standard approved for use in the United States employs the MPEG-2 transport stream format for packeting and multiplexing the video, audio and data signals.

An MPEG packet has an overall length of 188 bytes and includes a 4-byte header field and a variable length adaptation field which can vary in length from zero bytes to several bytes. The remainder of the packet is comprised of payload bytes. A DSS packet has an overall length of 130 bytes and includes a 3-byte header field and an optional variable length adaptation field of relatively-small length. The remainder of the DSS packet is comprised of payload bytes.

FIG. 22 is a flow chart which explains the general nature of the multiple data transport feature of the present invention. Each newly received data byte (block 103) is examined and qualified according to its position and value in its data packet (block 125). The examined byte is then tagged with a plural-bit tag (block 126), the value of the tag being determined by the results of the qualifying process (block 125). The resulting tagged byte is then passed on as a qualified byte (block 124). In the present embodiment, the process described by FIG. 22 is performed by the TS input unit 52 shown in FIG. 9. The qualification and tagging of the received data bytes is performed by the parsers 137 and 138.

Referring to FIG. 23, there is shown a detailed flow chart for a representative implementation of the method of FIG. 22. This multiple transport method of FIG. 23 enables the conditional access module 17 to handle any of the MPEG, ATM and DSS transport stream formats. Each incoming data byte is qualified according to its position and value within its packet. This qualification mechanism attaches a 5-bit tag to each

data byte, which tag contains all the information required for further processing of the byte. The qualification of each new byte starts with block 103 of FIG. 23, which block represents the reception of the new byte. The byte is first examined to determine if it is a header byte (block 104). If it is, a determination is then made as to whether it contains channel identification (ID) data (block 105). If the answer is yes, the byte is assigned a 3-bit tag portion having a value of "011" (block 106). If it is not a channel ID, then the byte is assigned a 3-bit tag portion having a value of "010" (block 107). Note that the total tag is a 5-bit tag. The purpose of the other two bits will be described shortly.

If the determination of block 104 determines that the new byte is not a header byte, then the byte undergoes a series of further non-header byte tests. The first test, represented by block 108, is to determine whether the byte is a null byte. If yes, it is assigned a 3-bit tag having a code of "000", as indicated by block 109. If the answer is no, then the byte proceeds to an adaptation field test represented by block 110. If the byte is an adaptation field byte, then it is assigned a tag value of "101", as represented by block 111. If it is not an adaptation field byte, then the test of block 112 is performed to determine whether or not it is a table identification (ID) byte. If yes, the byte is assigned a 3-bit tag having a value of "110", as represented by block 113. If no, the byte is examined per block 114 to determined whether it is a section length indicator byte. If yes, it is assigned a 3-bit tag value of "001", as indicated at block 115. If no, the byte proceeds to the payload decision block 116. Since this is the only alternative left, the byte is determined to be a payload byte and is given a 3-bit tag portion having a value of "111", as indicated at block 117.

After assignment of the initial 3-bit portion of its tag, the newly received byte is tested as indicated by decision block 118, to determine whether its data is scrambled or clear. If scrambled, a fourth bit in the tag, namely, the SCR bit is set to 1. If not scrambled, the SCR bit is set to 0. The byte is then tested as indicated by block 121 to determine whether it is the last byte of either a header field or a payload field. If it is a last byte, the LTB bit (the fifth bit in the 5-bit tag) is set to 1 (block 122) and if not, the LTB bit is set to 0 (block 123). This completes the qualification process and the

qualified output byte at step 124 is now in condition for further processing in the conditional access module 17.

The qualification process of FIG. 23 produces a stream of output bytes which are no longer dependent on the particular transport stream format which brought them to the conditional access module 17. Thus, the conditional access module 17 is enabled to process a variety of different transport stream formats in an efficient manner with minimal complication. And while the described implementation supports the MPEG, DSS and ATM transport stream formats, it can be readily extended to handle other packet-type or cell-type transport structures.

Fig. 24 is a timing diagram for the serial to parallel conversion performed in the serial to parallel converter 132 of Fig. 9. The MI CLOCK wave form represents the sampling clock signal used in the converter 132. The MDI wave form represents the serial data train. The MIVAL wave form is a valid signal which is at the high level when the current data is valid. The MISTRT wave form is start signal and is active high during the first byte of the serial data stream. The SBE and SSE wave forms are used to indicate whether the most significant bit (MSB) is the first or last bit of the byte and to indicate whether sampling is done on the rising or trailing edge of the MI CLOCK signal.

The serial to parallel converter 132 is comprised of a shift register and the incoming serial data is shifted into one end of the register and shifted across the length of the register. When all bits of a data byte are resident in the register the register stages are read out in a parallel manner to provide the output parallel data signal.

Figs. 25-28 show the timing diagrams for the different cases according to whether the most significant bit (MSB) is the first or last bit in the byte and whether sampling is done on the rising edge or the falling edge of the MI CLOCK signal. Fig. 25 shows the case where MSB is the first bit of the byte and sampling is done on the rising edge of the MI CLOCK signal. This sampling represents the moment when the shift register stages are read out in parallel. Fig. 26 represents the case where the least significant bit (LSB) is the first bit in the byte. Or the Fig. 26 case the sampling is performed on the rising edge of the MI CLOCK signal. Fig. 27 represents the case where MSB is the first bit and sampling is done on the falling edge of the MI CLOCK

signal while Fig. 8 indicates the case where LSB is the first bit with the sampling being performed on the falling edge of the clock signal.

Fig. 29 is a timing diagram showing the data stream synchronization provided by registers 130-133 of Fig. 9. The TS-DATA IN wave form shows the time period during which a byte of data is resident in each of the registers 130-133. The TS-DATA OUT wave form shows the time period during which data is read out of the registers 130-133. These read out intervals are controlled by the TS-CLOCK-OUT wave form. The rising edge of each TS-CLOCK-OUT pulse marks the beginning of each read out interval. The setting of data into registers 130-133 is controlled by the TS-CLOCK-IN signal. Fig. 30 shows the alternative case where data is moved into the registers 130-133 on the falling edge of the TS-CLOCK-IN signal.

Referring now to Fig. 31 there is shown a block diagram of the first-in first-out (FIFO) buffer 135 of Fig. 9. This is a 192 byte buffer and is used to buffer the incoming data bytes (TS-DATA-IN). Fig. 32 is a state diagram for the operation of FIFO buffer 135 when data is being written into the buffer. State "0" is a read input data state during which the FIFO is ready to receive input data. State "1" is an input synchronization state during which internal flags are set and an internal counter is initialized. State "2" is an initialization state for the new packet. Wherein the FIFO is initialized and its pointer is set to the next FIFO cell. State "3" is the actual writing operation wherein the input data is written into the current FIFO cell. The FIFO pointer is moved to the next cell and the internal counter is decremented. State "4" is a previous packet null operation wherein the packet ready flag is set to receive the next packet. The abbreviations used in Fig. 32 are as follows: S denotes the TS-SYNCHRO-N signal; CI denotes the TS-CLOCK-IN signal; VI denotes the TS-VALID-IN signal; Ct denotes the counter interval; and PR denotes the packet ready signal.

Fig. 32A is a state diagram for FIFO 135 when data is being read out of the FIFO 135. During State 0 the data in the current FIFO cell is read. In State 1 the data is sent to the output and the FIFO pointer is moved to the next cell. In State 3 the packet null flag is reset and in State 3 the valid data flag is set. In State 4 the validation flag is reset if the data is not valid. BS denotes the synchronization bit for the byte system and PN denotes the packet null bit in the byte system.

Fig. 33 is a block diagram that is showing in greater detail the construction of the transport stream (TS) parser 137 of Fig. 9. As seen in Fig. 33, the parser 137 includes individual parsers 301, 302 and 303 for the individual ones. The DVB, DSS, and the ATM signal transmission formats. A multiplexer 302 connects the appropriate one of the parsers 301-303 to the data output line 305.

The other transport stream parser 138 of Fig. 9 is of this same construction as shown in Fig. 33.

Fig. 34 is a block diagram for the DVB parser 301 of Fig. 33. This DVB parser 301 is constructed to handle the MPEG packet format (Fig. 19) used by the DVB transmission protocol. Fig. 35 shows this MPEG packet format in greater detail. A complete MPEG packet is shown at 310. It is 188 bytes in lengths. Details of the 4 byte header portion are shown at 311. Wave form 312 is a scrambling indicator signal and a high level indicates that the pay load data is scrambled.

Fig. 36 is a block diagram of the DSS parser 302 of Fig. 33. Fig. 37 shows the details of the DSS packet format for the DSS signals. Fig. 37 also shows some of the output signals produced by the DSS parser 302. A complete 130 byte DSS packet is indicated at 320. The SCR signal indicates whether or not the pay load data is scrambled. A low level indicates no scrambling and a high level indicates that the pay load is scrambled. Fig. 38 shows a state diagram for the DSS parser 302. State "0" is a read input data state, State "1" is a start packet mode, State "2" is a test control flag mode, and States "3"-"5" are pay load handling modes. State "3" is for the first pay load byte, State "4" is for the intermediate bytes and State "5" is for the last pay load byte. As indicated by wave form 321 in Fig. 37 the last byte indicator is turned on in State "5".

Referring to Fig. 39 there is shown a block diagram for the ATM parser 303 of Fig. 33. This ATM parser 303 is adapted to handle the 53 byte ATM cell format shown in Fig. 21. Fig. 40 shows a state diagram for the ATM parser 303. State "0" is a read data input mode. State "1" is a pay load first byte mode in which an internal counter in the ATM parser 303 is incremented. State "3" is a state wherein the first 5 bytes are typed as a packet header. State "4" is a pay load state wherein the pay load bytes are typed as pay load bytes. The internal counter is also incremented once for each byte.

State "5" is a length mode wherein bytes 43 and 44 are typed as length bytes. State "6" is a last byte mode wherein the data is typed as a last byte. The symbol TA in Fig. 40 is an ATM trailer flag indicating if there is any trailer ATM in the pay load.

Fig. 41 is a timing diagram for the output stream interfacing for the signals appearing on each of the output lines of the TS input unit of Fig. 9. The interface is identical for both output buses. This interface is also the same as shown for the output of the TS parser 137 in Fig. 33. The selection parser 139 of Fig. 9 serving only to change the routing of the output signals. With reference to Fig. 41 the SPL-CLK-OUT signal is a sampling flock output signal. When this signal goes up to a high level it indicates that the data must be sampled on the next rising edge of the master clock signal.

Fig. 42 is a flow chart of multiple scrambling operation 419 according to one embodiment of the present invention. In particular, multiple scrambling 419 according to the present invention begins with host module pairing 420. Next, a copy protection scrambling mechanism is defined 421. Then, a scrambling session key change is undertaken 422. Finally, a new session key is loaded 423 in memory, followed by a repeat of changing 422 the scrambling session key. As shown in FIG. 12 descrambling employs an input data register 140 for receiving the TSin data stream from the multiplexer 76 of FIG. 10. The descrambler 80 includes a set of eight decoders 141-148 for descrambling any one of the following encryption formats: DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB. Other encryption formats can be accommodated by providing appropriate additional decoders.

A descramble format register 150 and an associated decoder 151 determine which one of the primary decoders 141-148 is activated to process the incoming data stream. Descramble format register 150 is loaded by way of the VPB bus with a plural-bit control signal which designates the decoder to be used. This control signal is decoded by the enable signal decoder 151 to activate one and only one of its output lines. Thus, only a selected one of the decoders 141-148 is activated or used for any given data transport stream. It is also necessary to load a session key register 152 with a descrambling session key which tells the selected one of decoders 141-148 how to descramble the incoming data stream. This descrambling key is loaded into register

152 by way of the VPB bus. Register 152, in turn, supplies the descrambling key to each of the decoders 141-148 and it is used by the decoder which is selected by the control signal in the descramble format register 150. The descrambled data stream appearing at the output of the selected one of decoders 141-148 is supplied to an output data register 153 to provide a clear or unscrambled output signal TSclear or TSc. Referring now to FIG. 13, there is shown the details of a representative form of construction for the copy protect scrambler 81 of FIG. 11. For the embodiment shown in FIG. 13, the descrambler 81 includes a set of three encoders 155, 156 and 157 for encoding the TSclear signal from descrambler 80 in accordance with any one of the following three encryption formats: DES-ECB, DES-CBC and DES-OFB. Other scrambling formats may be used if desired. Selection of a desired one of the encoders 155-157 is accomplished by means of a plural-bit 7 control signal which is loaded into a scramble format register 158. This control signal controls an enable signal decoder 159 to activate a select one of its output lines, which output lines individually run to different ones of the encoders 155-157. The scrambled data stream appearing at the output of the selected encoder is supplied to an output data register 160 to provide the copy protected output signal TSprotected or TSp. The actual scrambling process which is followed in the selected encoder is controlled by a plural-bit scrambling session key which is loaded into a session key register 161. This scrambling session key is obtained from the microprocessor unit 42 by way of the VPB bus.

Fig. 43 is a flow chart of multiple scrambling operation 429 according to another embodiment of the present invention. In particular, multiple scrambling 429 according to the present invention begins with a channel change 430. After the channel change, the network descrambling mechanism is defined 431. Then, a scrambling session key change is undertaken 432. Finally, a new session key is loaded 433 in memory, followed by a repeat of changing 432 the scrambling session key.

Fig. 44 is a flow chart of multiple scrambling operation 439 according to yet another embodiment of the present invention. In particular, multiple scrambling 439 according to the present invention begins with reception of a new qualified packet cell byte 440. Next, a determination is made as to whether the received qualified packet cell is scrambled or not 441. If the received qualified packet cell is not scrambled, then the

clear packet cell byte is output 442. If the received qualified packet cell is scrambled, then determination of full block status is made 443. If yes, then the full block is descrambled 444. Then, a determination is made with respect to copy protection 445. If the determination is negative, then the clear packet cell byte is output 442. If the full block determination 443 is negative, a short block determination is made 446. If the short block determination is affirmative, then short block descrambling is undertaken 442. If the short block determination is negative, a solitary block determination is made 451. If the solitary block determination is affirmative, then solitary block descrambling is undertaken 452. After short block descrambling 447 and after solitary block descrambling 452, a determination of copy protection desired is undertaken 445. If the copy protection determination is affirmative, then determination of full block status is made 448. If yes, then the full block is scrambled 449. Then, the scrambled packet cell byte is output 450. If the full block determination 448 is negative, a short block determination is made 453. If the short block determination is affirmative, then short block scrambling is undertaken 454. If the short block determination is negative, a solitary block determination is made 455. If the solitary block determination is affirmative, then solitary block scrambling is undertaken 456. After short block scrambling 454 and after solitary block scrambling 456, the scrambled packet cell byte is output 450.

While there have been described what are at present considered to be preferred embodiments of this invention, it will be obvious to those skilled in the art that various changes and modifications may be made therein without departing from the invention and it is, therefore, intended to cover all such changes and modifications coming within the true spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A method of real time adaptive descrambling and scrambling, comprising:

receiving data in data units;

determining an encryption state of the data;

in the case of unencrypted data, providing a clear output;

in the case of encrypted data, determining a unit size of the received data unit and performing a decrypting function in accordance with the unit size determined, thereby providing decrypted data;

determining if the decrypted data includes a copy protection indicia;

in the case of the decrypted data including the copy protection indicia performing an encryption function, said encryption function performed in accordance with the unit size determined, thereby providing encrypted data;

in the case of the decrypted data including the copy protection indicia outputting the encrypted data.

2. The method according to claim 1, comprising

pairing a selected host with a selected module;

selecting a desired scrambling format;

selecting a session key; and

loading a selected session key in a selected memory.

3. The method according to claim 1, comprising selecting a scrambling format from a group including DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB, wherein DVB means digital video broadcasting, DES means Data Encryption Standard, ECB means electronic code book, CBC means chain block cipher, and OFB means output feedback block.

4. The method according to claim 1, including processing broadcast signals for scrambling.

5. The method according to claim 1, including processing burst signals for scrambling.

6. A method of real time adaptive scrambling, comprising:
pairing a selected host with a selected module;
selecting a desired scrambling format; and
selecting a session key.

7. The method according to claim 6, comprising selecting a scrambling format from a group including DES-ECB, DES-CBC, and DES-OFB.

8. The method according to claim 6, including processing broadcast signals for scrambling.

9. The method according to claim 6, including processing burst signals for scrambling.

10. A method of real time adaptive descrambling, comprising:
pairing a selected host with a selected module;
selecting a desired descrambling format; and
selecting a session key.

11. The method according to claim 10, comprising selecting a descrambling format from a group including DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB, wherein DVB means digital video broadcasting, DES means Data Encryption Standard, ECB means electronic code book, CBC means chain block cipher, and OFB means output feedback block.

12. The method according to claim 10, including processing broadcast signals for descrambling.

13. The method according to claim 10, including processing burst signals for descrambling.

14. The method according to claim 10 including descrambling with an input data register for receiving an TSin data stream from a multiplexer.

15. The method according to claim 10 including using a descrambler having a plurality of decoders for descrambling any one of the following encryption formats: DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB, wherein DVB means digital video broadcasting, DES means Data Encryption Standard, ECB means electronic code book, CBC means chain block cipher, and OFB means output feedback block.

16. The method according to claim 15 including using a descramble format register and an associated decoder to select which one of the plurality of decoders to activate for processing incoming data.

17. The method according to claim 16 including using a descramble format register for loading by way of a VPB bus with a plural-bit control signal which designates the decoder to be used.

18. The method according to claim 17 wherein said control signal is decoded by an enable signal decoder to activate an output line.

19. The method according to claim 10 including loading a session key register with a descrambling session key which tells the selected one of the decoders how to descramble the incoming data stream.

20. The method according to claim 19 including loading a descrambling key into a register by way of a VPB bus.

21. The method according to claim 20 including supplying the descrambling key to each of the plurality of decoders.

22. The method according to claim 21 including selecting a decoder with a control signal in a descramble format register; and

producing a descrambled data stream at the output of a selected one of a plurality of decoders to an output data register.

23. A copy protect scrambler comprising:

a scramble format register configured to hold a plural-bit control signal; and

a plurality of encoders for each encoding a TSclear signal from a descrambler in accordance with any one of a selected plurality of encryption formats, said plurality of encoders being configured to be individually selected by a plural-bit control signal loaded into said scramble format register.

24. The copy protect scrambler according to claim 23 including an enable signal decoder configured to activate a selected one of a plurality of output lines individually connected to different ones of the encoders.

25. The copy protect scrambler according to claim 23 configured to produce a scrambled data stream at the output of a selected encoder.

26. The copy protect scrambler according to claim 23 wherein scrambling is controlled by a plural-bit scrambling session key which is loaded into a session key register.

27. The copy protect scrambler according to claim 26 wherein the scrambling session key is obtained from a microprocessor by way of a VPB bus.

28. A method of multiple scrambling comprising:
making a channel change;
selecting a network descrambling mechanism;
making a scrambling session key change; and
loading a new session key.

29. A method of multiple scrambling according to claim 28, comprising:
receiving a qualified packet cell byte; and
determining whether the received qualified packet cell is scrambled, and if the received qualified packet cell is not scrambled, then outputting a clear packet cell byte.

30. A method of multiple scrambling comprising:
receiving a qualified packet cell byte; and
determining whether the received qualified packet cell is scrambled, and if the received qualified packet cell is not scrambled, then outputting a clear packet cell byte.

31. A method of multiple scrambling according to claim 30, wherein if the received qualified packet cell is scrambled, then a determination of full block status is made.

32. A method of multiple scrambling according to claim 31, wherein if full block status is determined, a full block is descrambled.

33. A method of multiple scrambling according to claim 31, wherein if the full block determination is negative, a reduced size block determination is made.

34. A method of multiple scrambling according to claim 30, comprising:
determining a copy protection status to assess whether copy protection is desired; and
if the copy protection status determination is negative, outputting a clear packet cell byte.

35. A method of multiple scrambling according to claim 34, comprising:

if the copy protection determination is affirmative, then a determination of block status is made; and

scrambling according to the block status.

36. A method of multiple scrambling according to claim 35, wherein if the block determination for a first size is negative, a shorter block determination is made; and

if the shorter block determination is affirmative, then the shorter block scrambling is undertaken.

37. A method of signal processing comprising:

receiving a qualified byte of data;

determining whether the received qualified byte is scrambled; and

if the received qualified byte is not scrambled, then a corresponding clear byte is output.

38. A method of signal processing according to claim 37, wherein a determination is made with respect to copy protection to assess whether copy protection is desired; and

if the determination is negative as to whether copy protection is desired, then a clear byte is output.

39. A method for enabling a conditional access module to handle any of a plurality of transport stream formats, said method comprising:

qualifying received data bytes according to its position and value within a packet;

attaching a multibit tag to each received data byte containing information required for further processing of the byte;

selecting a desired scrambling format; and

selecting a session key.

40. The method according to claim 39 further comprising examining each byte to determine if it is a header byte.

41. The method according to claim 39 further comprising determining whether the byte contains channel identification data.

42. The method according to claim 39, including performing an adaptation field test.

43. The method according to claim 39, including determining whether the byte is a payload byte.

44. The method according to claim 39 including determining whether the data in the byte is scrambled or clear.

45. The method according to claim 39 including producing a stream of output bytes which are no longer dependent on the particular transport stream format in which they arrived at the conditional access module.

46. A system for enabling a conditional access module to handle any of a plurality of transport stream formats, said multiple transport system comprising:

a qualification mechanism for processing received data bytes according to position and value within a packet;

a tagging mechanism for applying a multibit tag to each received data byte, containing information required for further processing of the byte;

a scramble format register configured to hold a plural-bit control signal; and

a plurality of encoders for each encoding a TSclear signal from a descrambler in accordance with any one of a selected plurality of encryption formats, said plurality of encoders being configured to be individually selected by a plural-bit control signal loaded into scramble format register.

47. The system according to claim 46 including:

an enable signal decoder configured to activate a selected one of a plurality of output lines individually connected to different ones of the encoders; and

the system configured to produce a scrambled data stream at the output of a selected encoder.

48. The system according to claim 46 wherein scrambling is controlled by a plural-bit scrambling session key which is loaded into a session key register.

49. The system according to claim 44 wherein the scrambling session key is obtained from a microprocessor by way of a VPB bus.

50. The system according to claim 46 including a mechanism for examining each byte to determine if it is a header byte.

51. The system according to claim 46 further comprising a mechanism for determining whether the byte contains channel identification data.

52. The system according to claim 46, including a mechanism for performing an adaptation field test.

53. The system according to claim 46 including a mechanism for determining whether the byte is a payload byte.

54. The system according to claim 46 including a mechanism for determining whether the data in the byte is scrambled or clear.

55. The system according to claim 46 including a mechanism producing a stream of output bytes which are not dependent on the particular transport stream format in which they arrived at the conditional access module.

56. The system according to claim 46 configured to receive input transport streams formatted according to MPEG, DSS and ATM transport stream formats.

57. The system according to claim 46 configured to receive packet-type and cell-type transport structures.

58. A method for handling any of a plurality of transport stream formats, said method comprising:

qualifying received data bytes according to its position and value; and

attaching a tag to each received data byte to indicate whether a qualified data byte is scrambled and whether it is to be copy protected.

59. A system capable of receiving a plurality of different transport stream formats, such mechanism comprising:

a qualifying mechanism for receiving and qualifying incoming data bytes according to their positions and values in their plural-byte data packets;

a tagging mechanism for assigning a plural-bit tag to each data byte, such tag having a unique value determined by the results of the qualifying process performed by the qualifying mechanism; and

a scramble format register configured to hold a plural-bit control signal.

60. A system comprising:

a plurality of receivers configured for communication with one or more broadband signal transmission sources producing signals in a selected transport stream format; and

a security mechanism configured to select a received signal transport streams for removal of a network distribution security layer therefrom according to whether the secure stream received is a full block, a short block, or a solitary block.

61. The system according to claim 60, wherein said network security mechanism applies content protection to predetermined signal streams.

62. The system according to claim 60 further including a plurality of decoders which are configured to select one or more of the signal streams and to decode each selected stream to recreate desired video, audio and data signals which are, in turn, supplied to one or more display units or one or more recording units.

63. The system according to claim 60 wherein said security mechanism is configured to examine received signals to determine their types.

64. The system according to claim 60 wherein said security mechanism is configured to control descrambling operation of received signals.

65. A set-top system comprising:

a plurality of receivers configured for reception of a secure stream from one or more broadband signal transmission sources; and

a security mechanism connected to each of said plurality of receivers, said security mechanism configured to remove the network distribution security layers therefrom, wherein said plurality of receivers and said security mechanism is located within a network specific set-top structure, and is configured to determine whether the secure stream received is a full block, a short block, or a solitary block.

66. A set-top system according to claim 65 wherein said security mechanism is configured to be renewable and removable from said network specific set-top structure; and

said security mechanism is a conditional access module which is a removable plug-in type element which is adapted to be plugged into a cooperating receptacle or socket in a host set-top box.

67. The set-top system according to claim 66 wherein the set-top box functions are located inside the containment of a television receiver cabinet which houses a display unit or picture tube; and

said security mechanism is adapted to plug into a cooperative receptacle.

68. A system comprising:

a plurality of receivers configured for communication with one or more broadband signal transmission sources producing signals in a selected transport stream format; and

a security mechanism connected to each of said plurality of receivers, said security mechanism configured to select one or more of the received signal transport streams and to remove the network distribution security restrictions therefrom.

69. The communication system according to claim 68 wherein each of said plurality of receivers includes an in-band channel and an out-of-band channel, which are adapted to receive incoming signals from a remote broadcasting station.

70. The communication system according to claim 68 wherein said in-band and out-of-band channels are connected with a filter bank configured to detect predefined digital patterns within received signals and to react thereto for establishing connections with appropriate ones of predetermined software applications.

71. The communication system according to claim 68 further including a smart card channel configured to enable communications with at least a single applications program.

72. In a digital signal receiving system for receiving encrypted digital data signals, the combination comprising:

input circuitry for receiving a digital data signal which is scrambled in accordance with a particular one of a plurality of different data encryption formats;

a control mechanism for supplying a control signal identifying the particular encryption format of the received signal;

a descrambling mechanism responsive to the control signal for descrambling the received data signal to provide a clear copy of the received data signal;

a scrambling mechanism for receiving the clear copy data signal;

a copy protection control mechanism for activating the scrambling mechanism for causing the scrambling mechanism to produce a copy protected scrambled data signal; and

circuitry for supplying the copy protected scrambled data signal to an end user utilization mechanism.

73. A digital signal receiving system in accordance with Claim 72 wherein the receiving system is a digital television receiving system and the data signals are television signals.

74. A digital signal receiving system in accordance with Claim 73 wherein the end user utilization mechanism includes a television display mechanism for producing visual images.

75. A digital signal receiving system in accordance with Claim 73 wherein the end user utilization mechanism is a video tape recorder.

76. A digital signal receiving system in accordance with Claim 72 wherein the received data signal is scrambled in accordance with a first data encryption format and the scrambling mechanism produces a scrambled data signal which is scrambled in accordance with a second data encryption format.

77. A digital signal receiving system in accordance with Claim 76 wherein the first data encryption format is a selected one of a DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC and 3DES-OFB, wherein DVB means digital video broadcasting, DES means Data Encryption Standard, ECB means electronic code book, CBC means chain block cipher, and OFB means output feedback block format and the second data encryption format is a DES format.

78. A digital signal receiving system in accordance with Claim 72 wherein the scrambling mechanism produces a scrambled data signal which is scrambled in accordance with an encryption format which is different from the encryption format of the received signal.

79. A digital signal receiving system in accordance with Claim 72 wherein the received data signal is scrambled in accordance with a particular one of eight different data encryption formats and the scrambling mechanism produces a copy protected scrambled data signal which is scrambled in accordance with a particular one of three different data encryption formats.

80. A digital signal receiving system in accordance with Claim 72 wherein the scrambling sequence for the received data signal is controlled by a scrambling key and the receiving system includes a scrambling key mechanism for supplying a replica of the received signal scrambling key to the descrambling mechanism for controlling the descrambling process therein.

81. A digital signal receiving system in accordance with Claim 72 and including a scrambling key mechanism for supplying a scrambling key to the copy protection scrambling mechanism for controlling the scrambling sequence therein.

82. A digital signal receiving system in accordance with Claim 72 wherein the descrambling mechanism comprises:

a plurality of decoder mechanisms for descrambling data signals having a plurality of different data encryption formats; and

a decoder selection mechanism responsive to the format identifying control signal for selecting the particular decoder mechanism which is used to descramble the received data signal.

83. A digital signal receiving system in accordance with Claim 72 wherein:
the copy protection scrambling mechanism includes a plurality of encoder mechanisms for scrambling the clear copy data signal in accordance with different data encryption formats; and

the copy protection control mechanism includes an encoder selection mechanism for selecting the particular encoder mechanism which is used to scramble the clear copy data signal.

84. A method for trans-scrambling bytes of received information, comprising:
decrypting a byte which is encrypted with a first type of encryption; and
re-encrypting said byte with a second type of encryption.

85. A method of processing bytes of information, comprising:
receiving a qualified byte;
determining whether the byte is scrambled; and
if not scrambled, passing the unscrambled byte as a clear byte without attempting encryption or copy protect scrambling actions.

86. A method of descrambling received bytes of information received over a selected channel; comprising:
selecting a channel for receipt of audio and/or video information;
determining the network descrambling mechanism for a selected channel from a predetermined set of candidate types of descrambling mechanisms; and
determining a descrambling session key to enable descrambling operation.

87. The method according to claim 86 further descrambling the byte according the determined mechanism and key.

88. The method according to claim 86 including further rescrambling with a selected copy protection scrambling mechanism.

89. The method of rescrambling descrambled information, comprising:

pairing a selected conditional access module or card with a selected host set top box module;

selecting a copy protect mechanism; and

determining a scrambling session key.

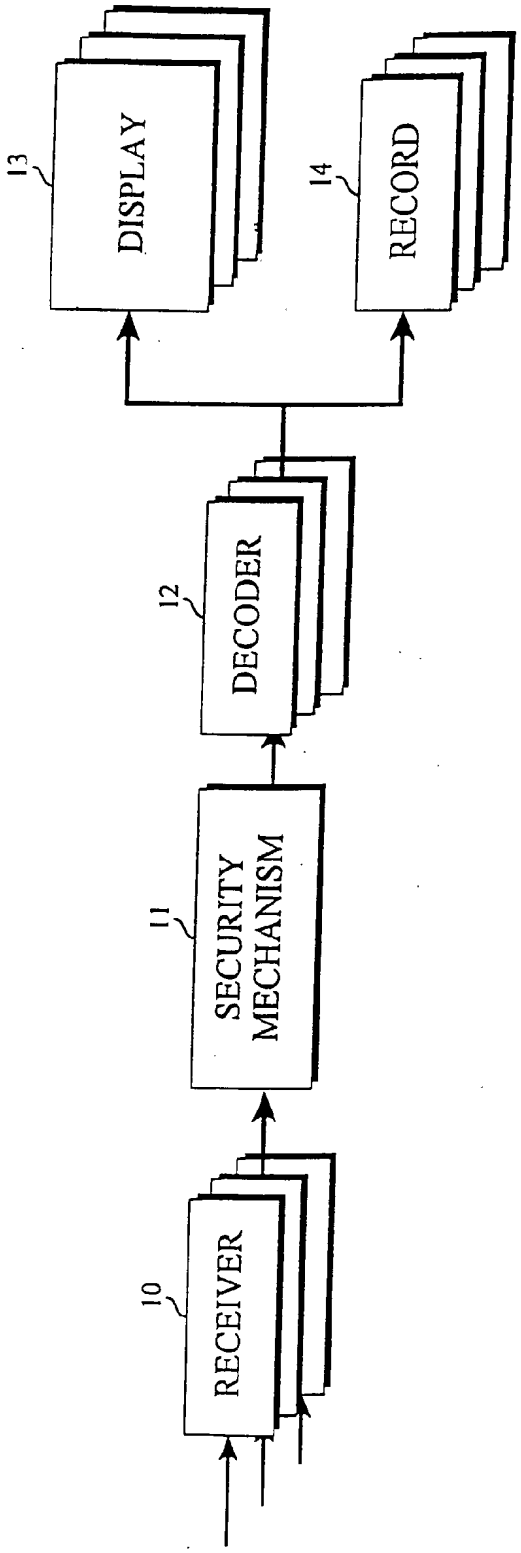

RECEIVER
10
SECURITY MECHANISM
11
DECODER
12
DISPLAY
13
RECORD
14

Fig. 1

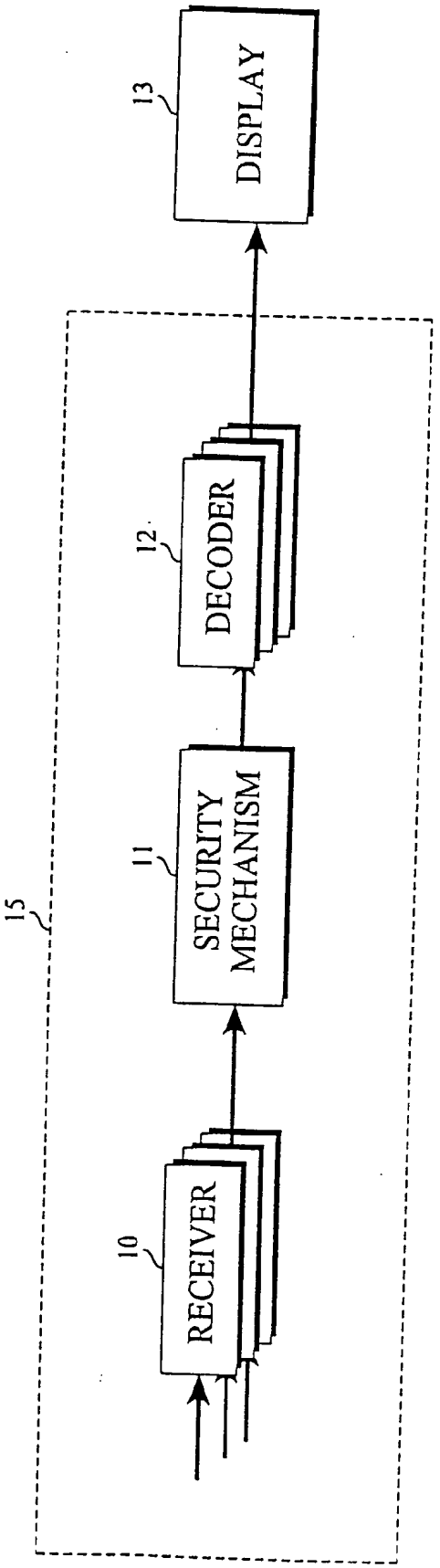

15
10
RECEIVER
11
SECURITY MECHANISM
12
DECODER
13
DISPLAY

Fig. 2A

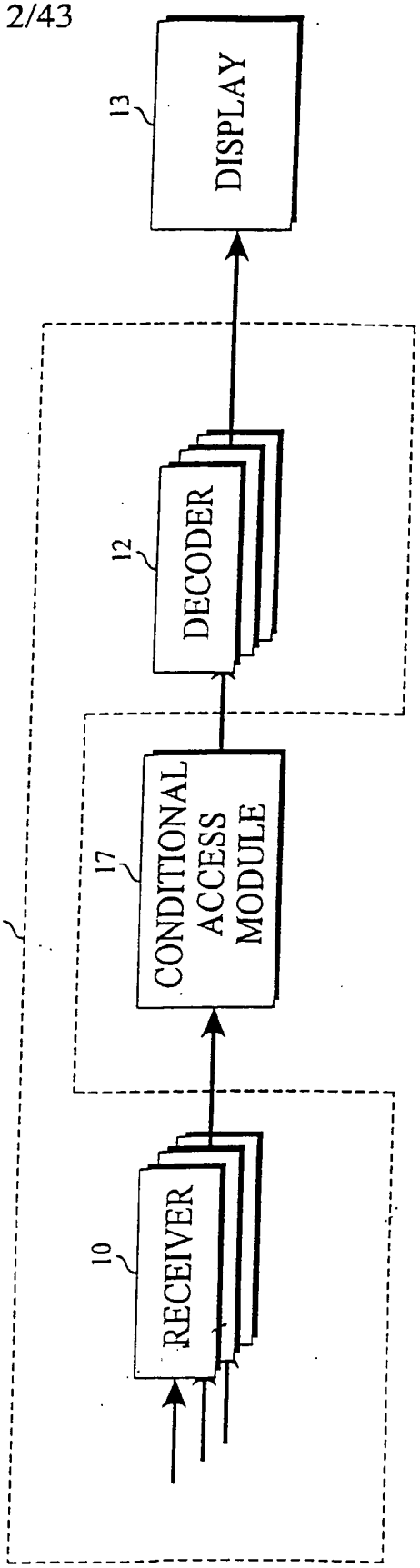

16
10
RECEIVER
17
CONDITIONAL ACCESS MODULE
12
DECODER
13
DISPLAY

Fig. 2B

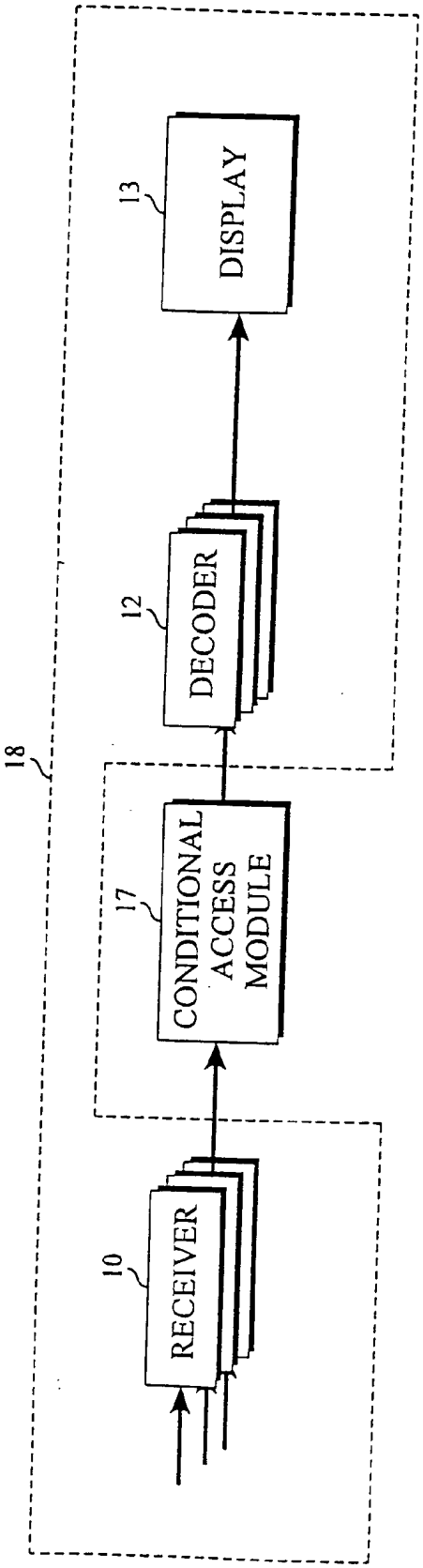

18
10
RECEIVER
17
CONDITIONAL ACCESS MODULE
12
DECODER
13
DISPLAY

Fig. 2C

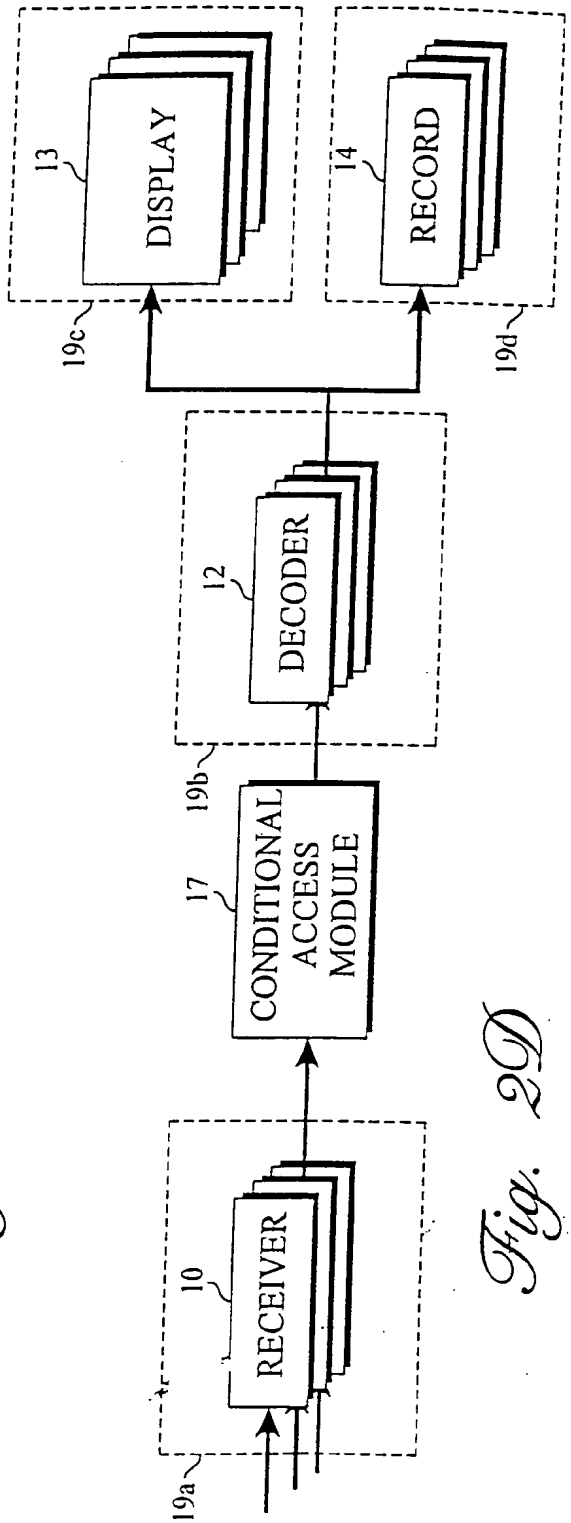

19a
10
RECEIVER
17
CONDITIONAL ACCESS MODULE
19b
12
DECODER
19c
13
DISPLAY
19d
14
RECORD

Fig. 2D

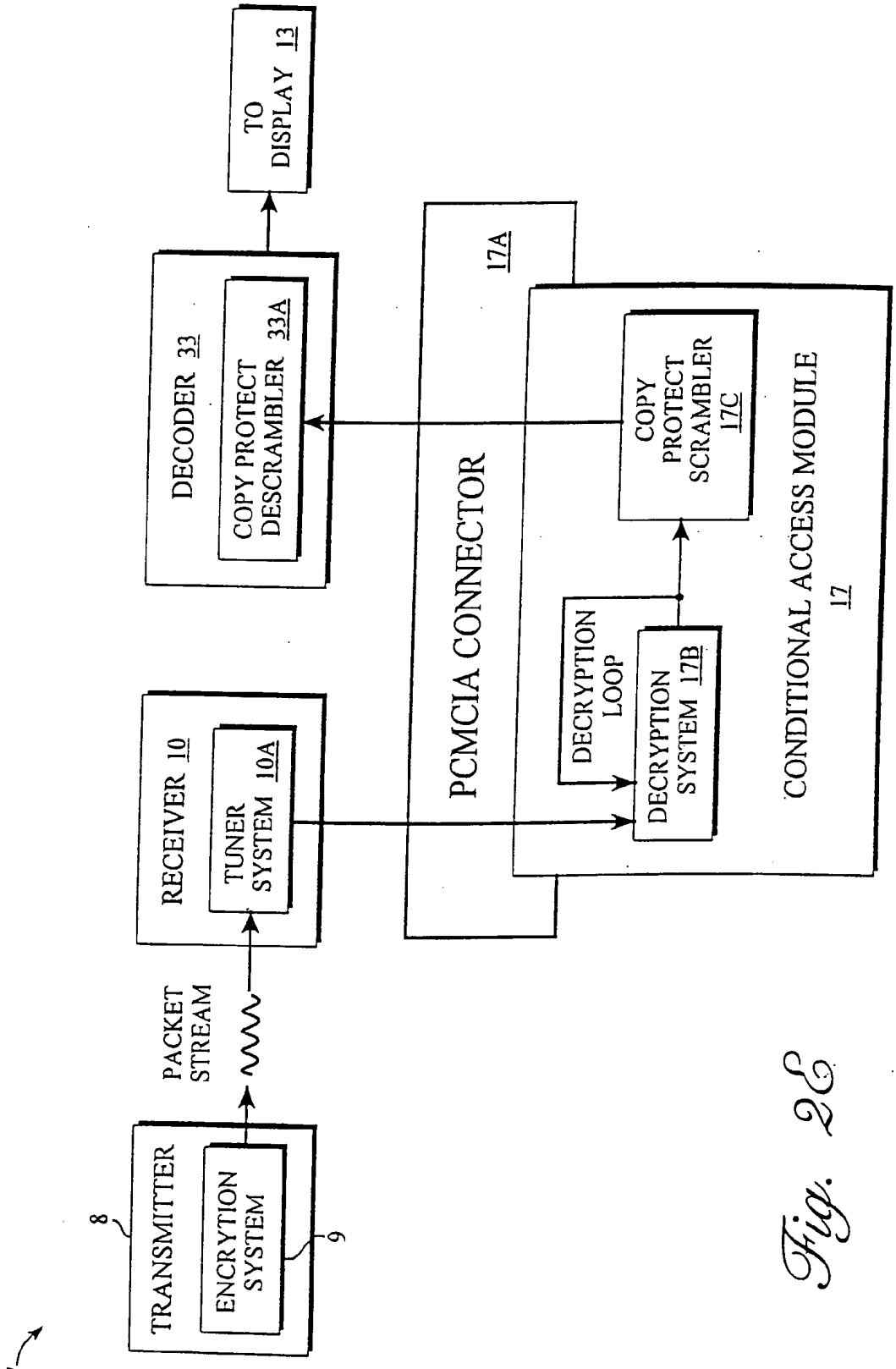

7
TRANSMITTER
8
ENCRYTION SYSTEM
9
PACKET STREAM
RECEIVER 10
TUNER SYSTEM 10A
DECODER 33
COPY PROTECT DESCRAMBLER 33A
TO DISPLAY 13
PCMCIA CONNECTOR
17A
CONDITIONAL ACCESS MODULE
17
DECRYPTION SYSTEM 17B
DECRYPTION LOOP
COPY PROTECT SCRAMBLER 17C

Fig. 2C

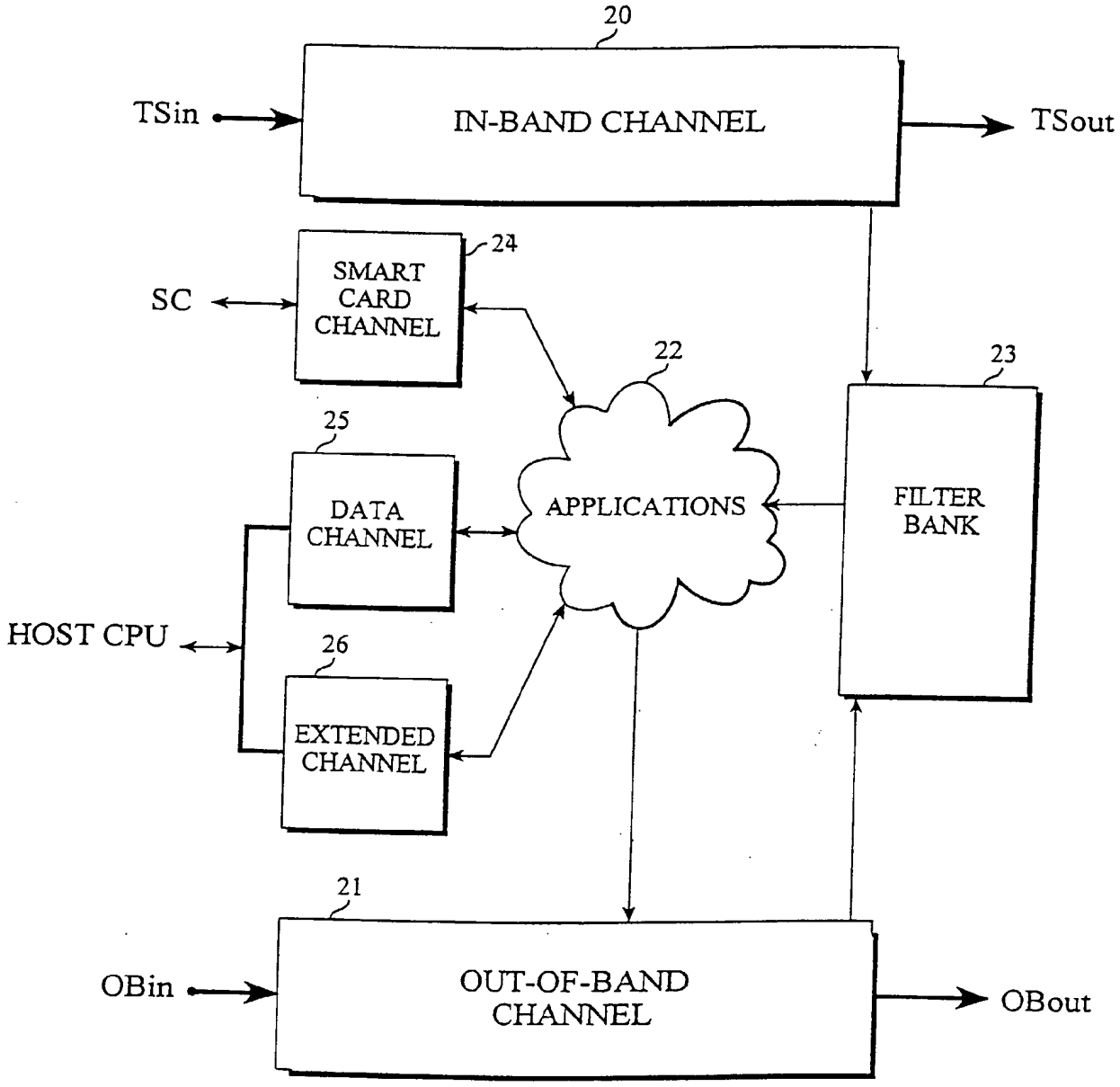

20
TSin
IN-BAND CHANNEL
TSout
24
SMART CARD CHANNEL
SC
22
23
25
DATA CHANNEL
APPLICATIONS
FILTER BANK
HOST CPU
26
EXTENDED CHANNEL
21
OBin
OUT-OF-BAND CHANNEL
OBout

Fig. 3

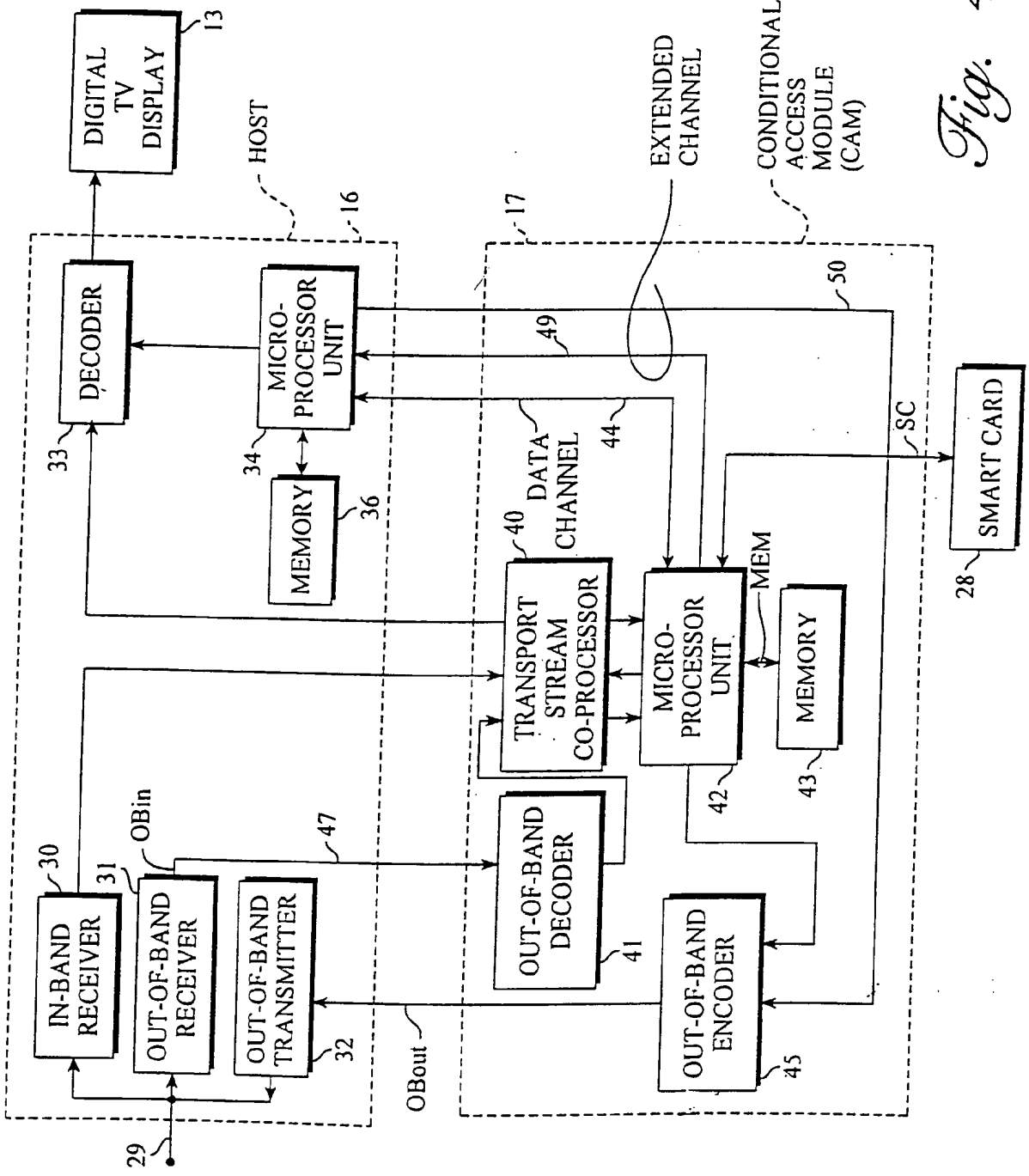

DIGITAL TV DISPLAY
13
HOST
16
17
EXTENDED CHANNEL
CONDITIONAL ACCESS MODULE (CAM)
DECODER
33
MICRO-PROCESSOR UNIT
34
MEMORY
36
49
50
44
DATA CHANNEL
40
SC
SMART CARD
28
TRANSPORT STREAM CO-PROCESSOR
MICRO-PROCESSOR UNIT
MEM
MEMORY
43
42
30
31
OBin
47
IN-BAND RECEIVER
OUT-OF-BAND RECEIVER
OUT-OF-BAND TRANSMITTER
32
OBout
OUT-OF-BAND DECODER
41
OUT-OF-BAND ENCODER
45
29

Fig. 4

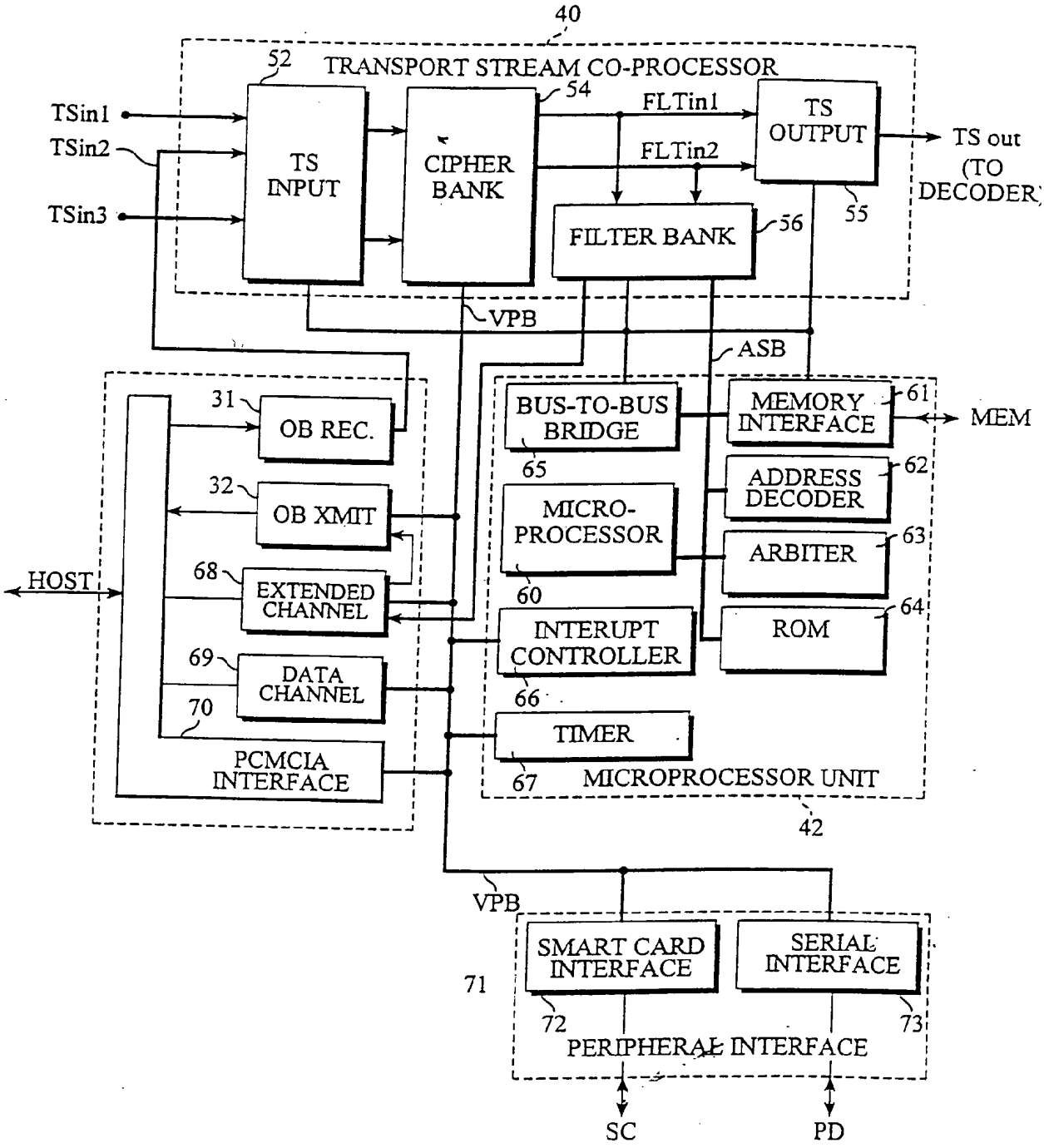

40
TRANSPORT STREAM CO-PROCESSOR
52
TSin1
TSin2
TSin3
TS INPUT
CIPHER BANK
54
FLTin1
FLTin2
TS OUTPUT
TS out (TO DECODER)
55
FILTER BANK
56
VPB
ASB
31
OB REC.
32
OB XMIT
HOST
68
EXTENDED CHANNEL
69
DATA CHANNEL
70
PCMCIA INTERFACE
BUS-TO-BUS BRIDGE
65
MICRO-PROCESSOR
60
INTERUPT CONTROLLER
66
TIMER
67
MEMORY INTERFACE
61
MEM
ADDRESS DECODER
62
ARBITER
63
ROM
64
MICROPROCESSOR UNIT
42
VPB
71
SMART CARD INTERFACE
SERIAL INTERFACE
72
73
PERIPHERAL INTERFACE
SC
PD

Fig. 5

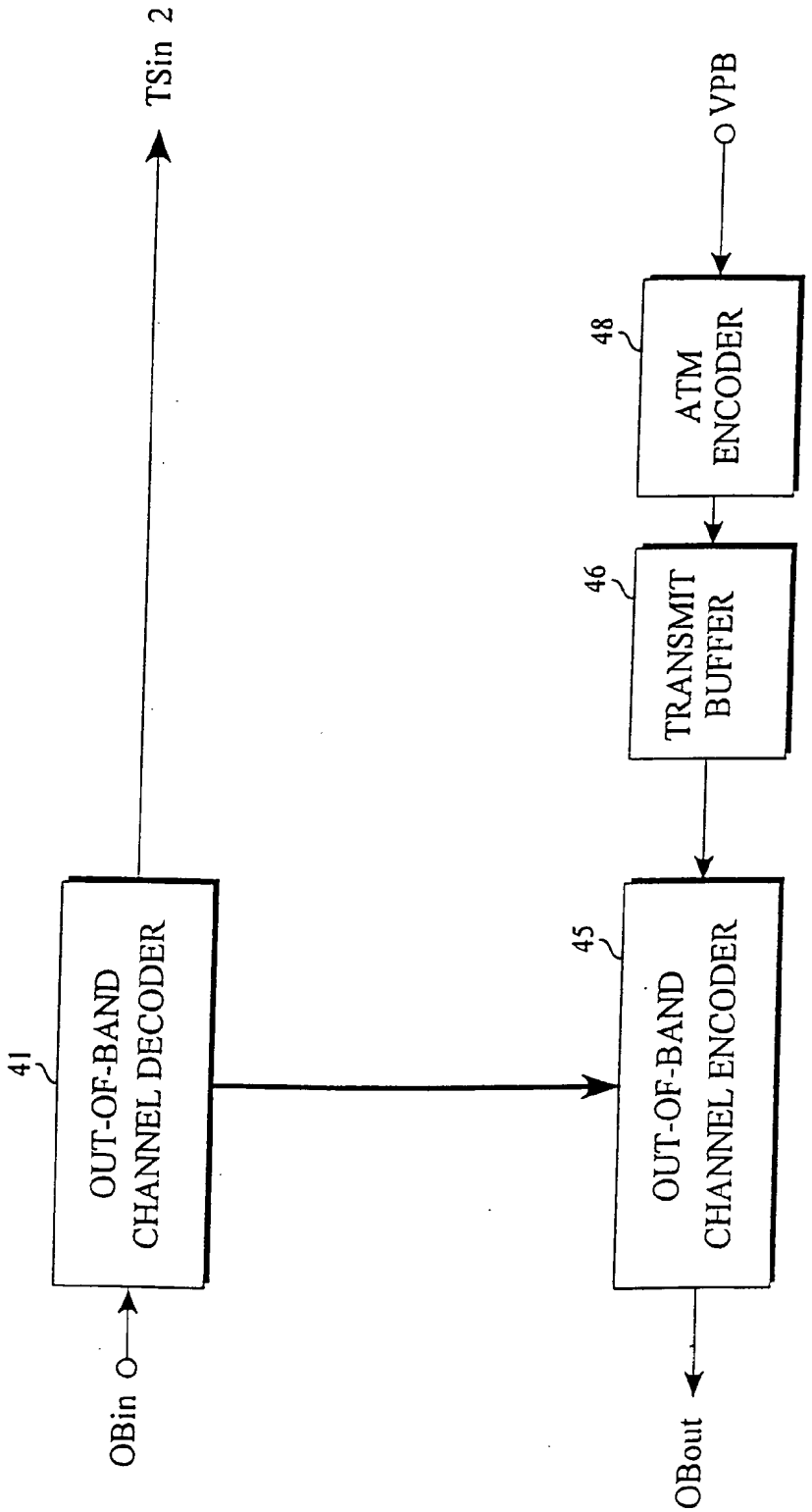

TSin 2
VPB
48
ATM ENCODER
46
TRANSMIT BUFFER
41
OUT-OF-BAND CHANNEL DECODER
45
OUT-OF-BAND CHANNEL ENCODER
OBin
OBout

Fig. 6

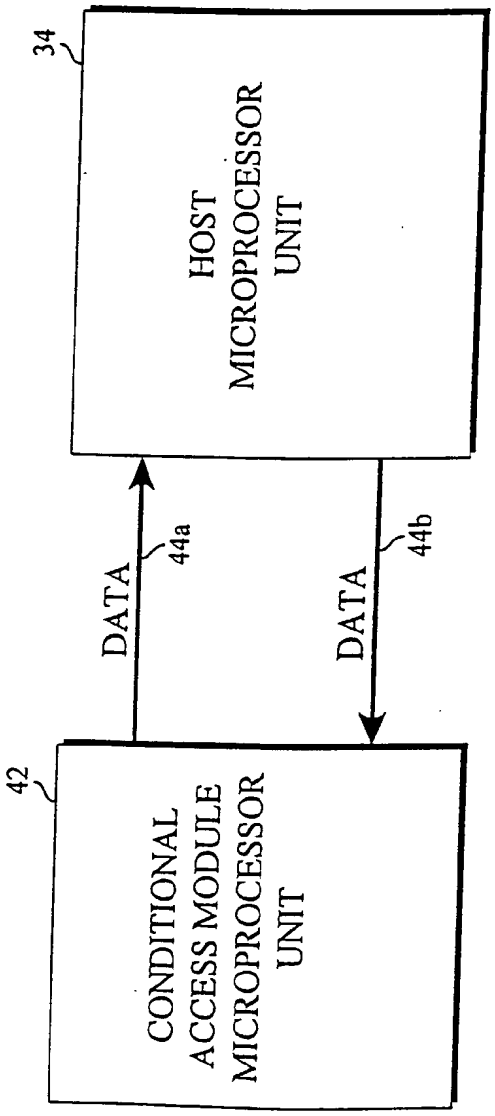

34
HOST MICROPROCESSOR UNIT
DATA
44a
DATA
44b
42
CONDITIONAL ACCESS MODULE MICROPROCESSOR UNIT

Fig. 7

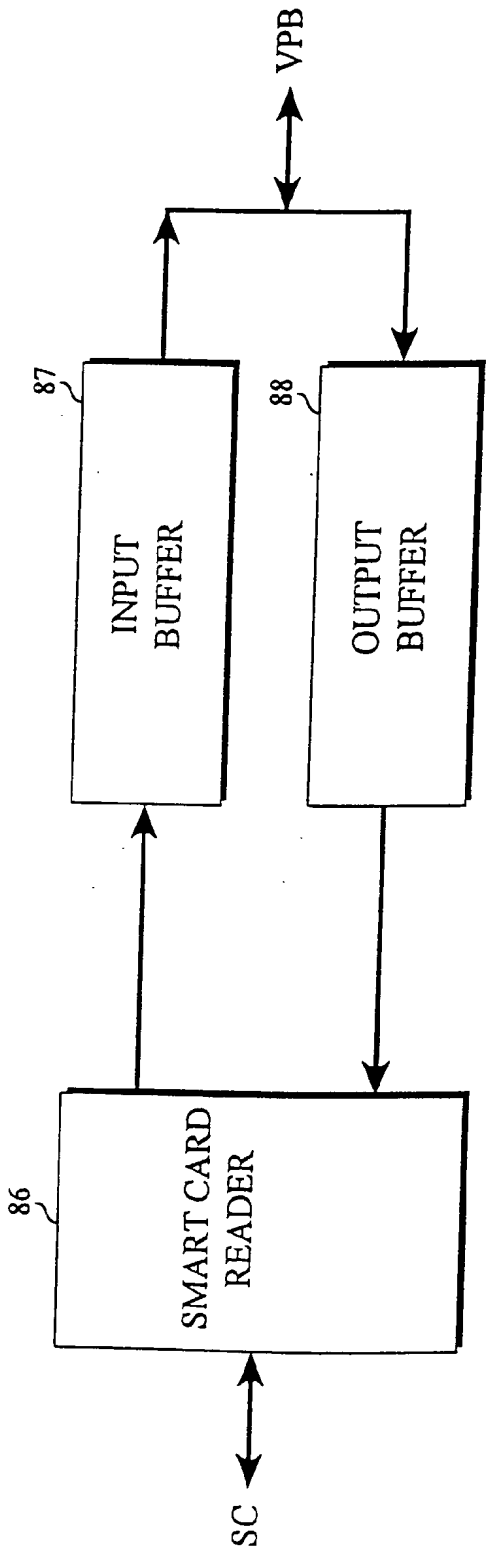


Fig. 8

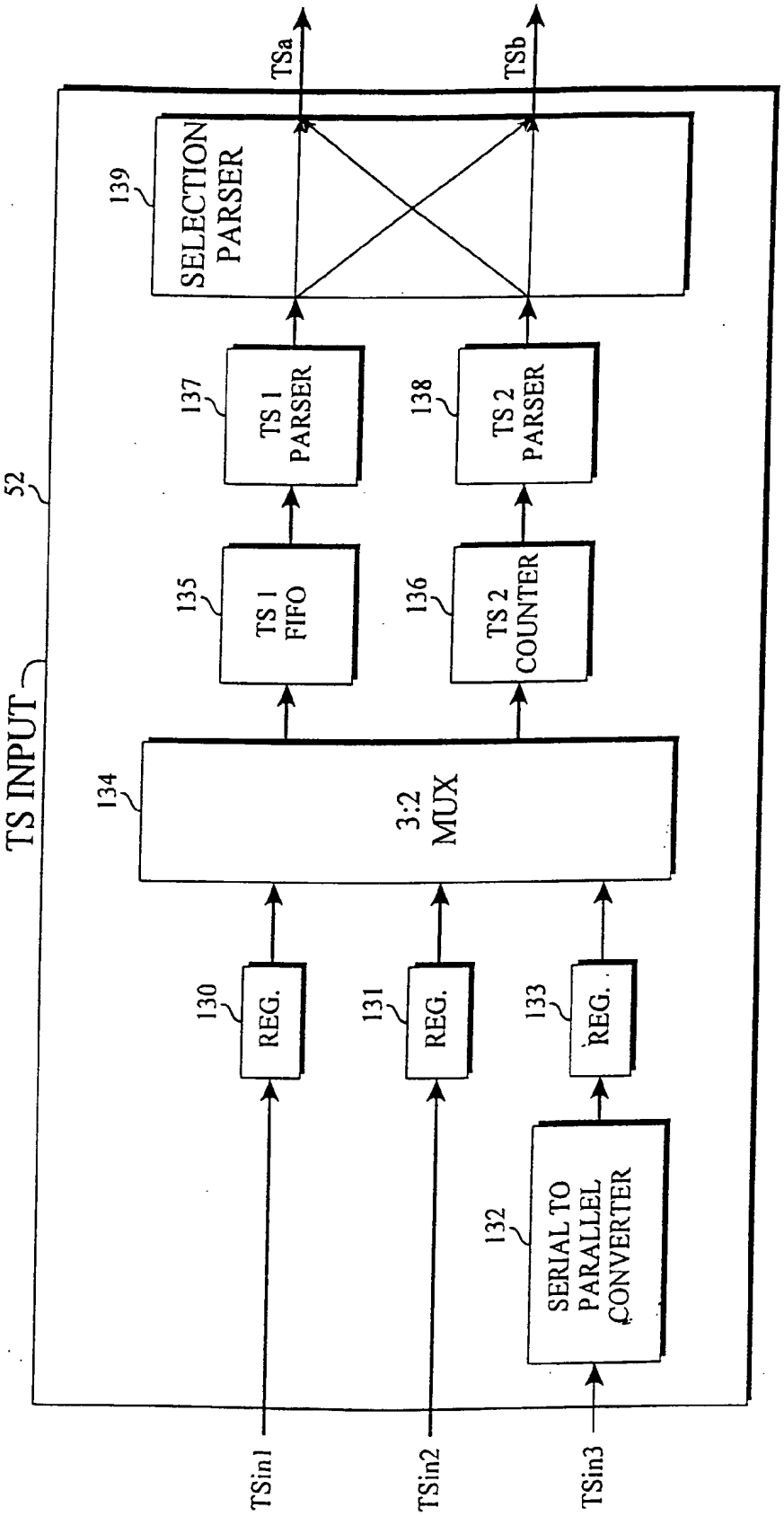

TSa
TSb
139
SELECTION PARSER
137
TS 1 PARSER
138
TS 2 PARSER
52
135
TS 1 FIFO
136
TS 2 COUNTER
TS INPUT
134
3:2 MUX
130
REG.
131
REG.
133
REG.
132
SERIAL TO PARALLEL CONVERTER
TSin1
TSin2
TSin3

Fig. 9

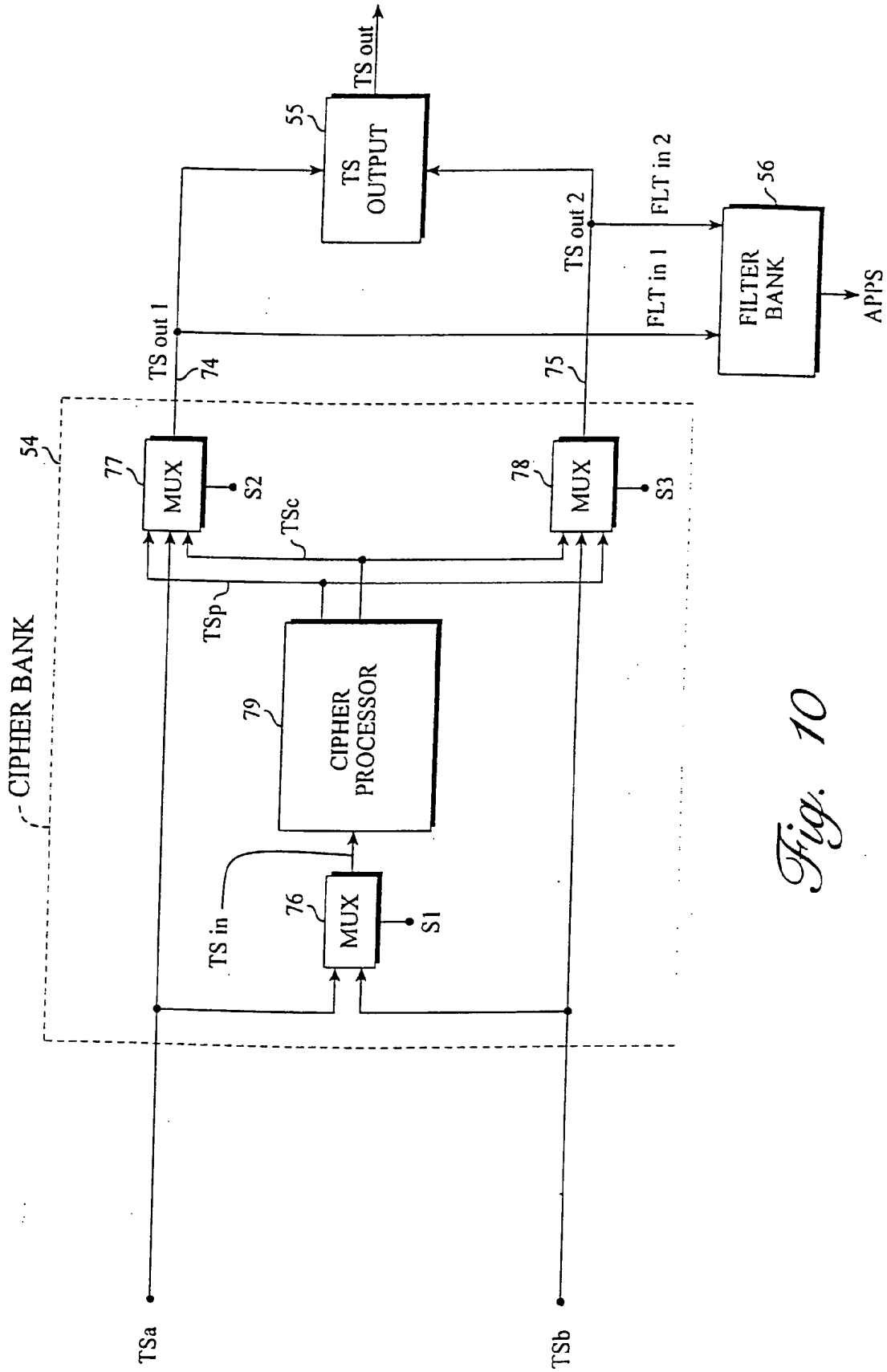

TS out
55
TS OUTPUT
TS out 2
FLT in 2
56
FLT in 1
FILTER BANK
APPS
TS out 1
74
75
54
77
MUX
S2
TSc
78
MUX
S3
TSp
CIPHER BANK
79
CIPHER PROCESSOR
TS in
76
MUX
S1
TSa
TSb

Fig. 10

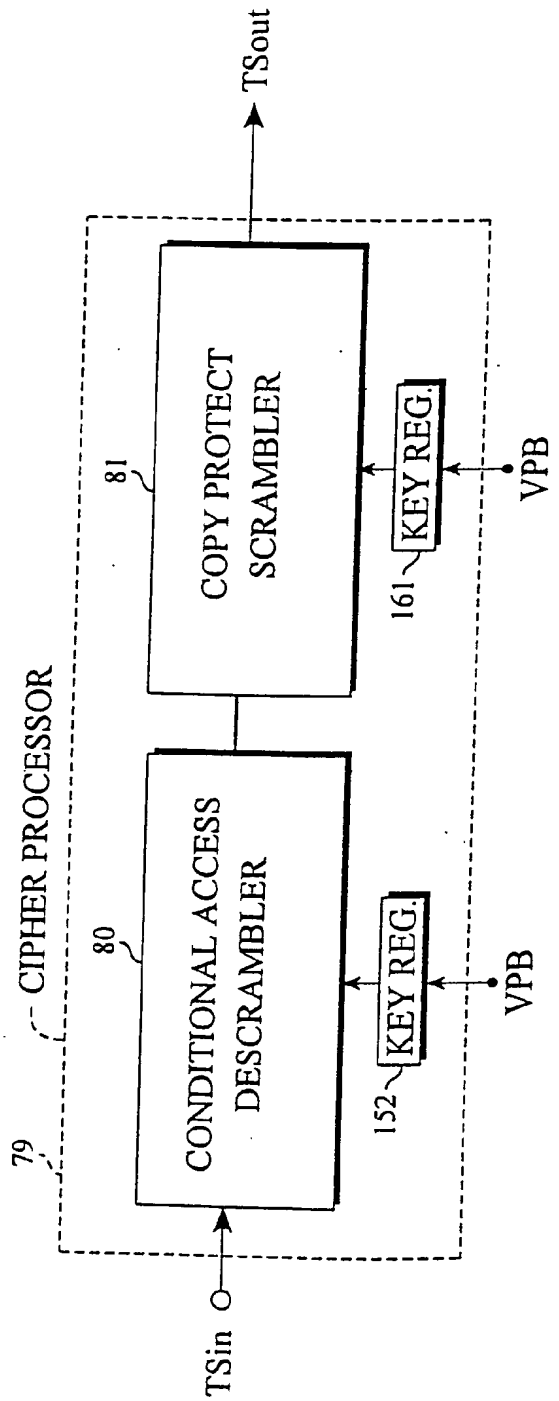

TSout
CIPHER PROCESSOR
79
CONDITIONAL ACCESS DESCRAMBLER
80
COPY PROTECT SCRAMBLER
81
KEY REG.
152
KEY REG.
161
VPB
VPB
TSin

Fig. 11

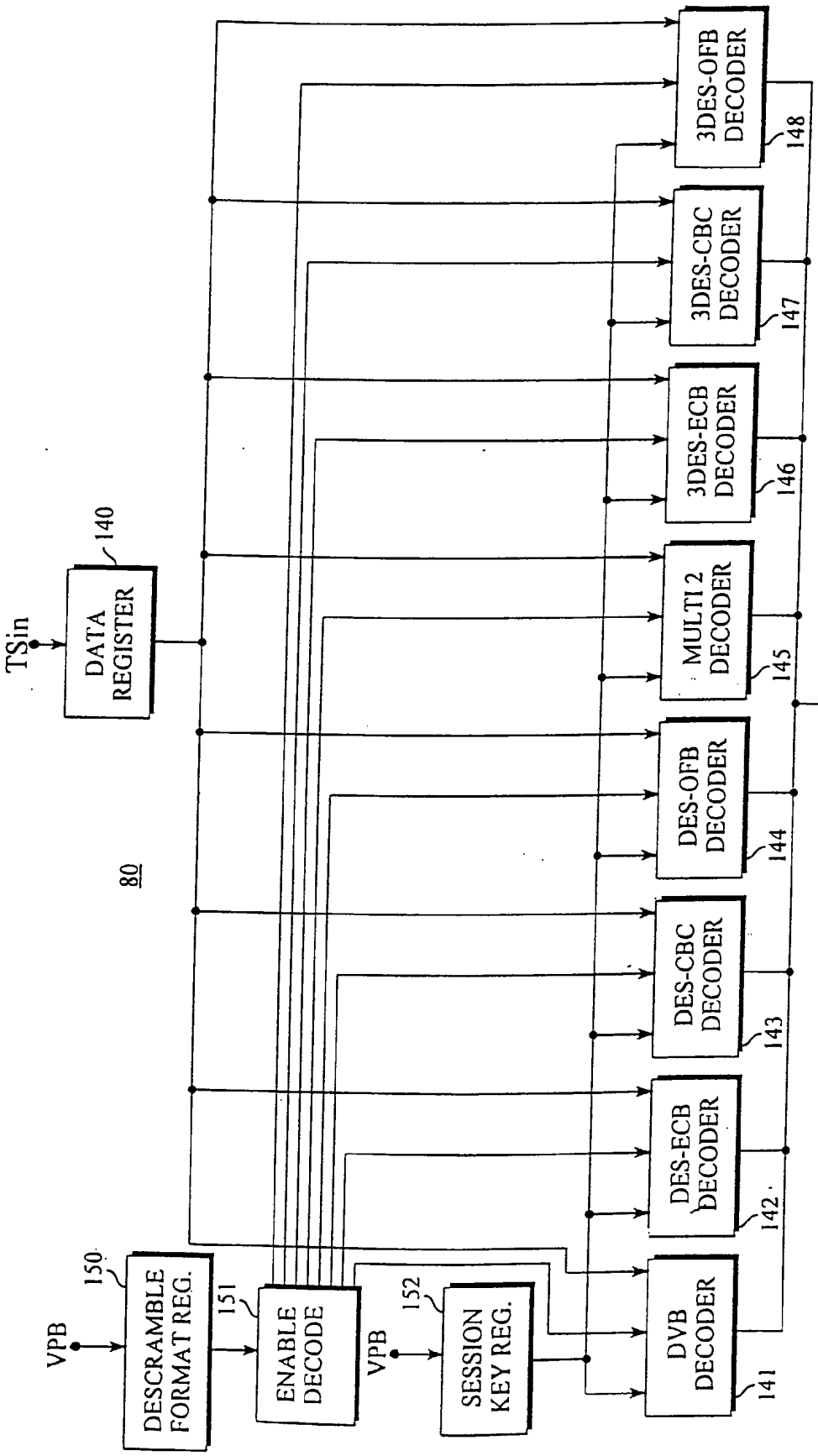

TSin
DATA REGISTER
140
80
VPB
150
DESCRAMBLE FORMAT REG.
151
ENABLE DECODE
VPB
152
SESSION KEY REG.
DVB DECODER
141
DES-ECB DECODER
142
DES-CBC DECODER
143
DES-OFB DECODER
144
MULTI 2 DECODER
145
3DES-ECB DECODER
146
3DES-CBC DECODER
147
3DES-OFB DECODER
148
DATA REGISTER
153
TSclear

Fig. 12

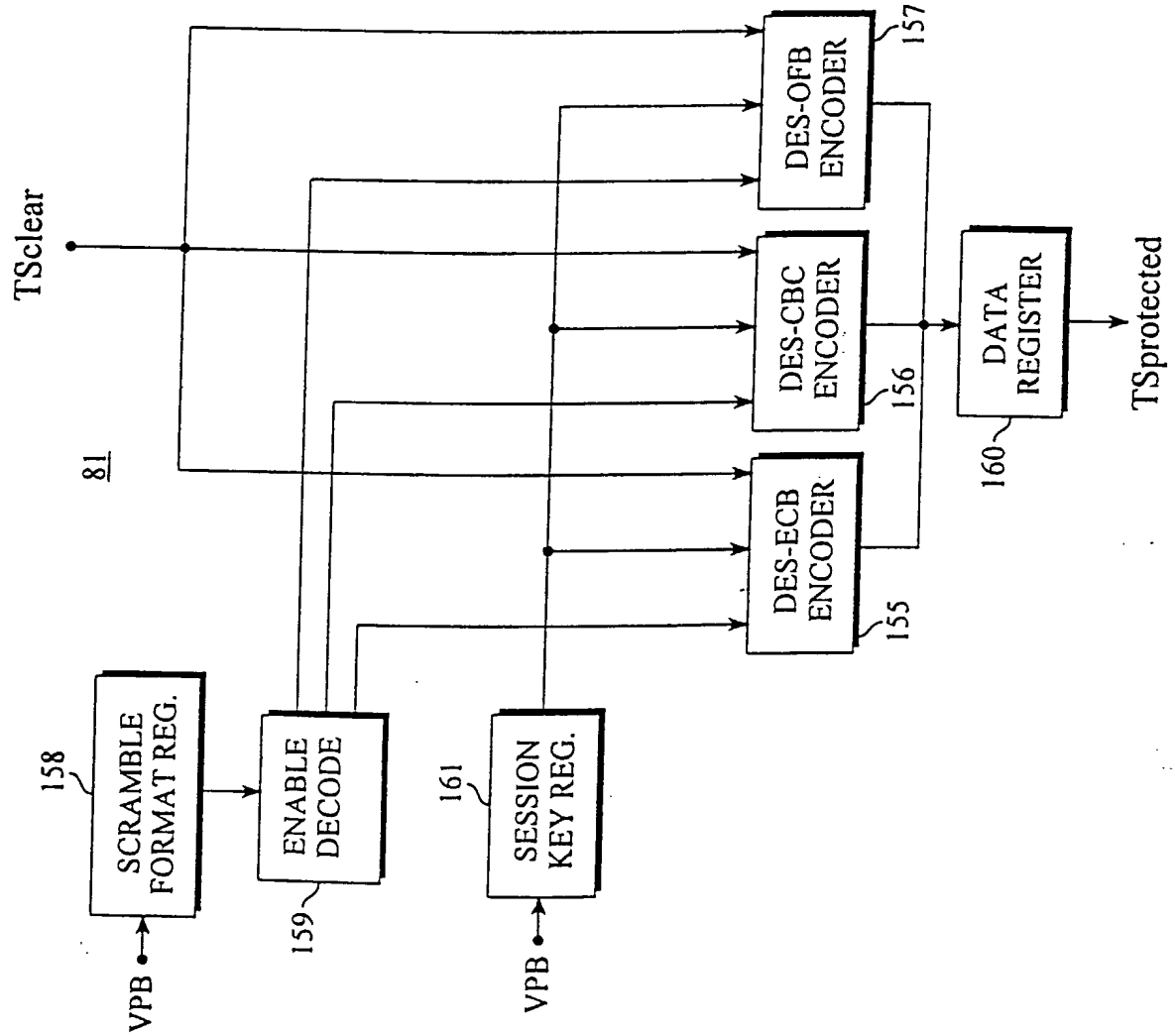

TSclear
81
DES-OFB ENCODER
157
DES-CBC ENCODER
156
DES-ECB ENCODER
155
DATA REGISTER
160
TSprotected
SCRAMBLE FORMAT REG.
158
ENABLE DECODE
159
SESSION KEY REG.
161
VPB
VPB

Fig. 13

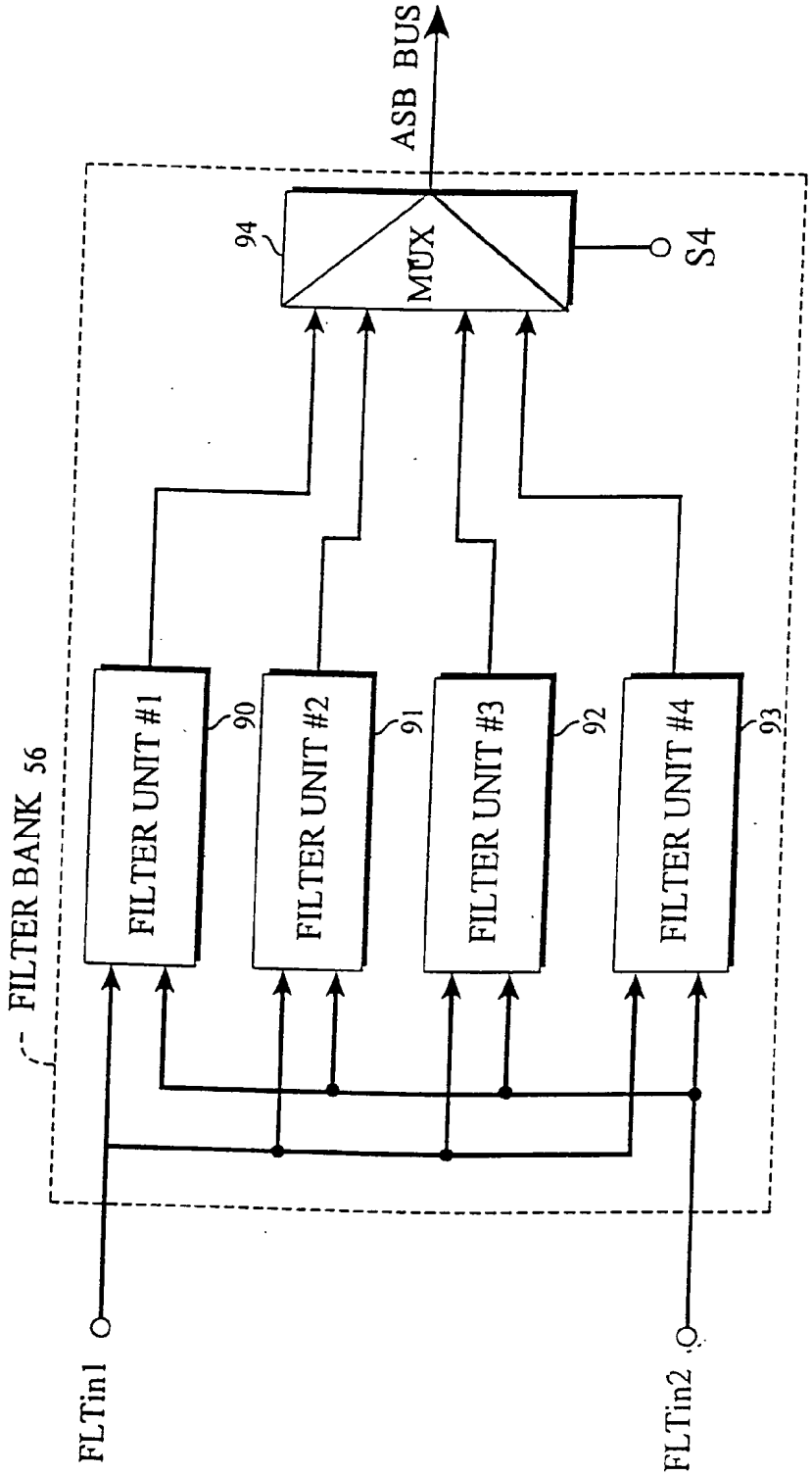

ASB BUS
94
MUX
S4
FILTER BANK 56
FILTER UNIT #1
90
FILTER UNIT #2
91
FILTER UNIT #3
92
FILTER UNIT #4
93
FLTin1
FLTin2

Fig. 14

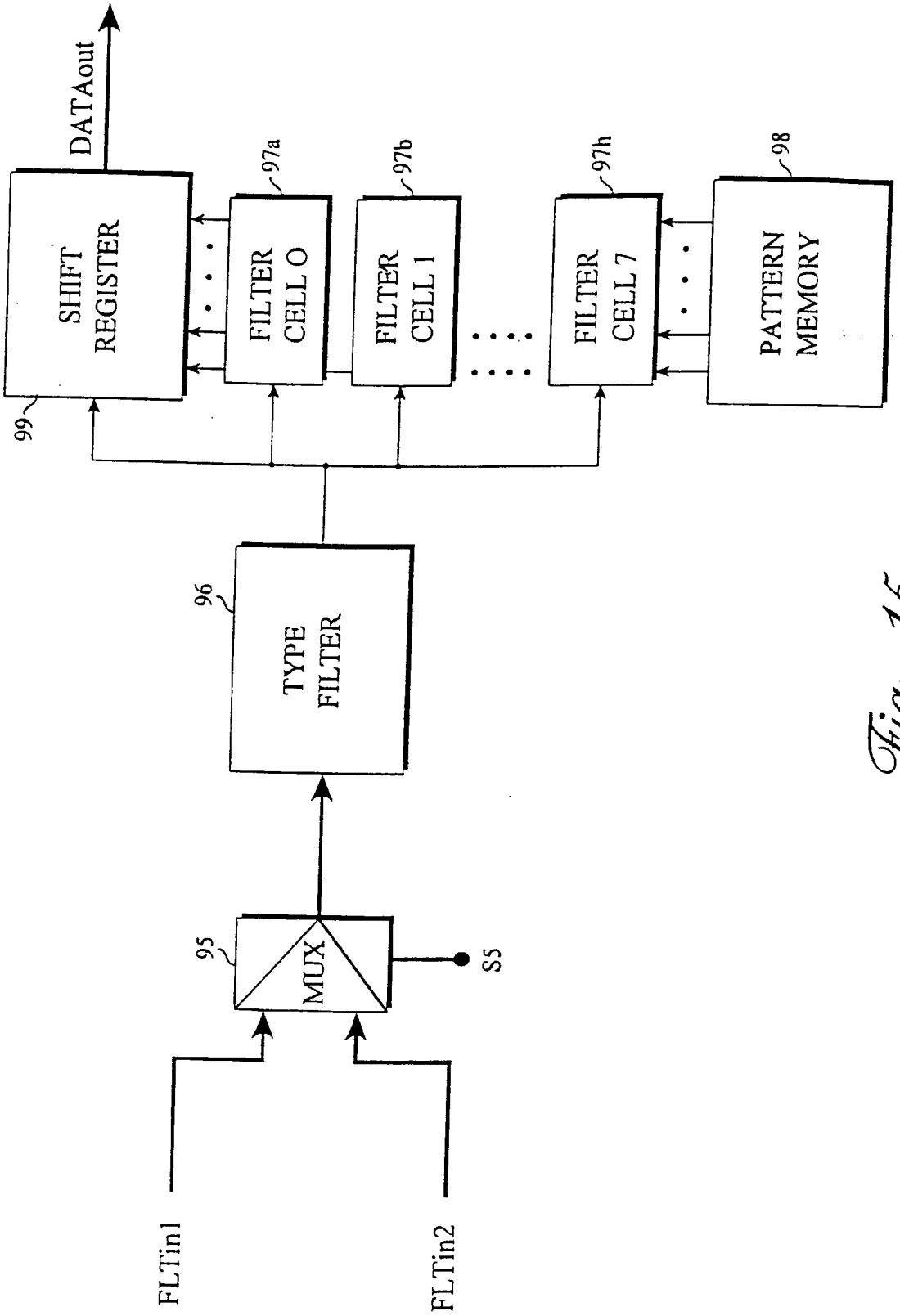

DATAout
SHIFT REGISTER
99
97a
FILTER CELL O
97b
FILTER CELL 1
97h
FILTER CELL 7
98
PATTERN MEMORY
96
TYPE FILTER
95
MUX
S5
FLTin1
FLTin2

Fig. 15

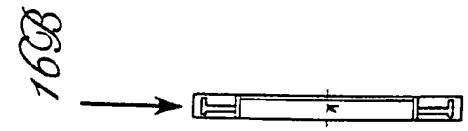


Fig. 16B

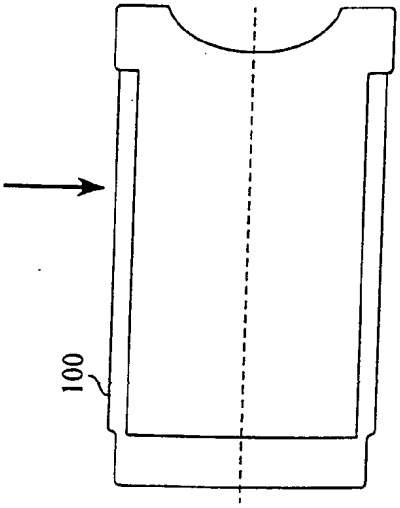


Fig. 16

Fig. 16C

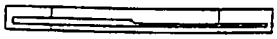


Fig. 16A

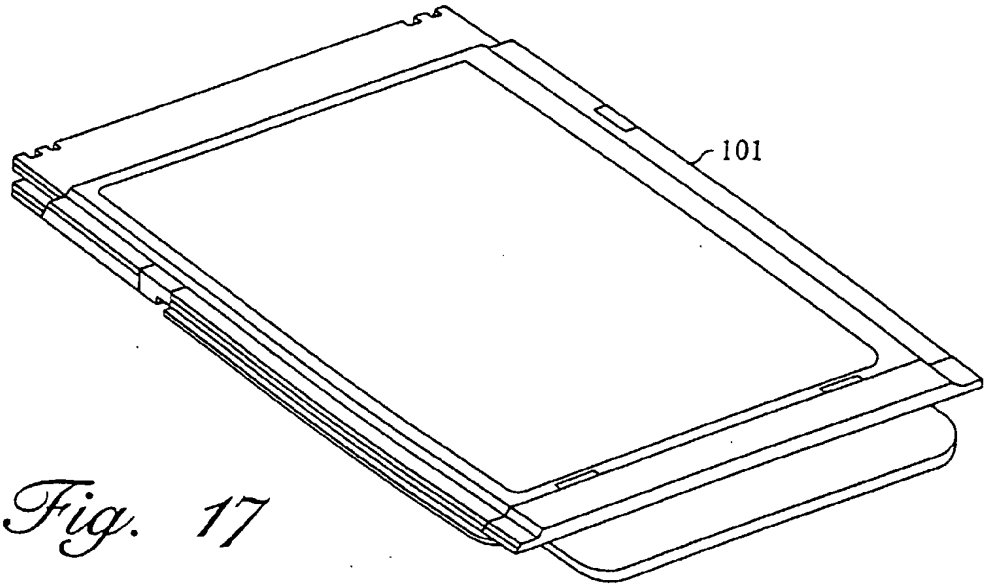


Fig. 17

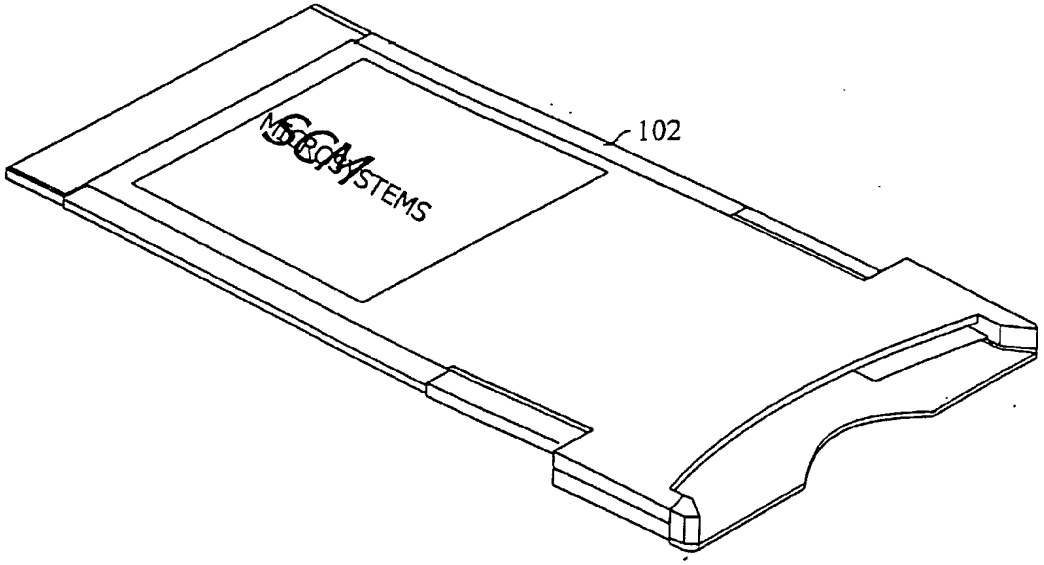


Fig. 18

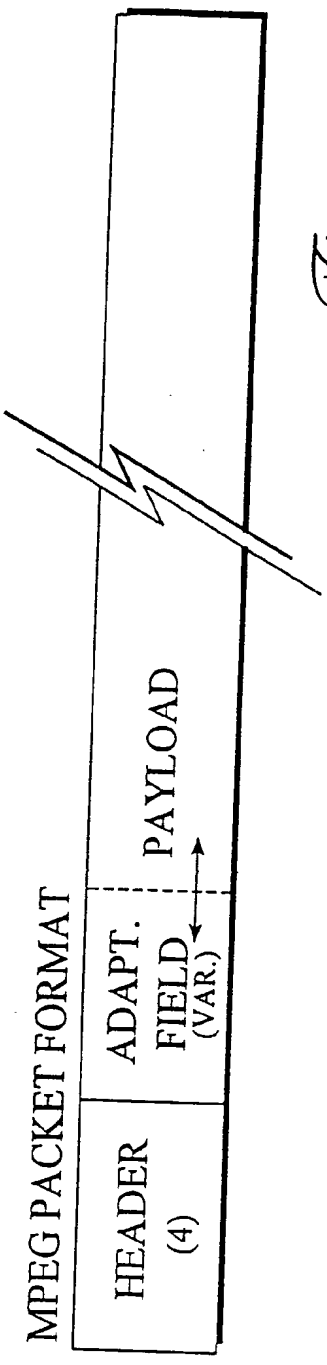


Fig. 19

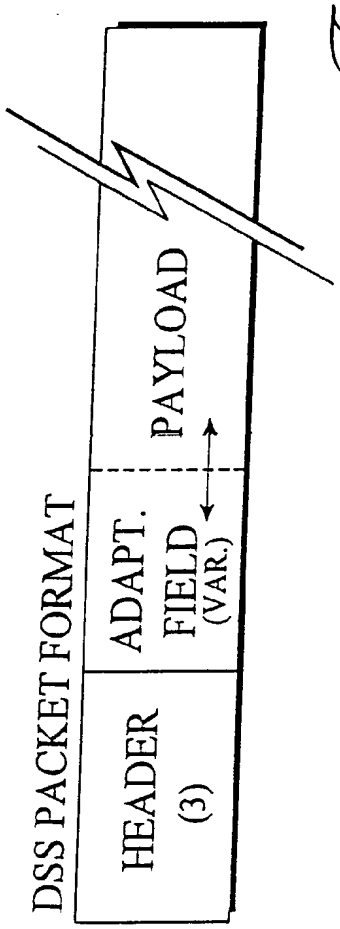


Fig. 20

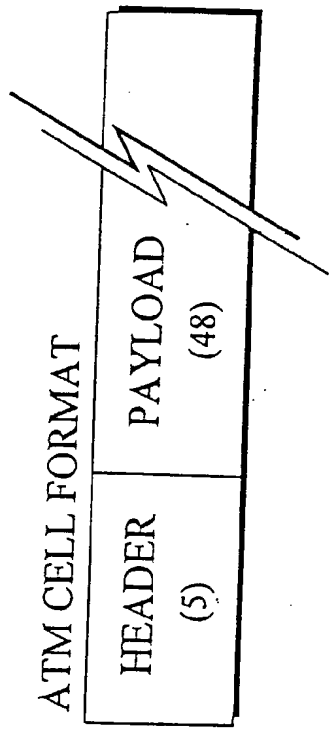


Fig. 21

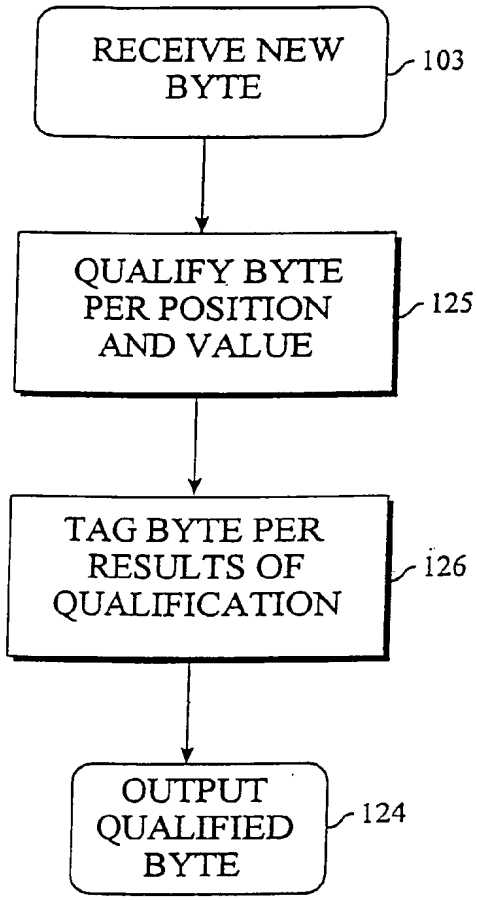

RECEIVE NEW BYTE
103
QUALIFY BYTE PER POSITION AND VALUE
125
TAG BYTE PER RESULTS OF QUALIFICATION
126
OUTPUT QUALIFIED BYTE
124

Fig. 22

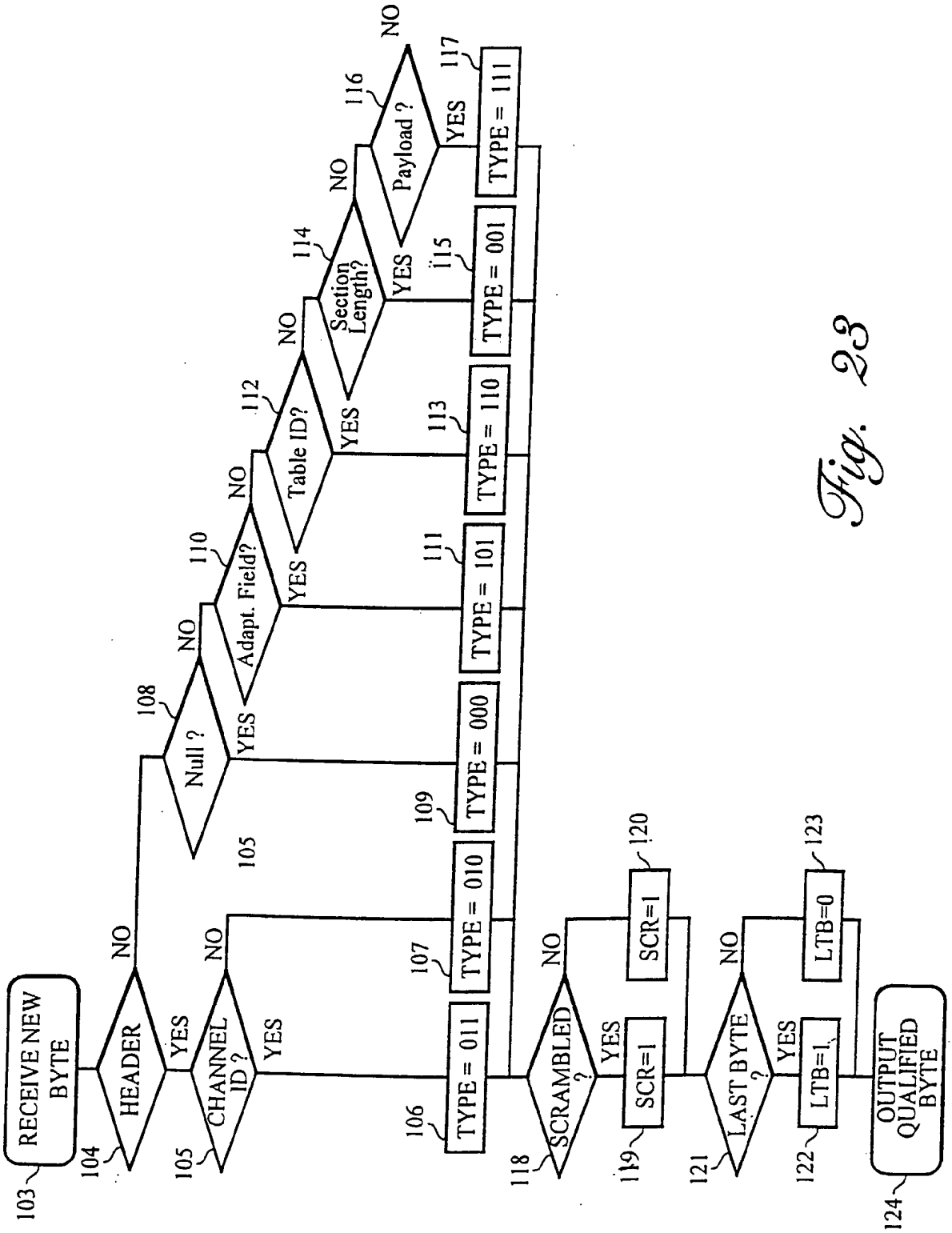

RECEIVE NEW BYTE
103
HEADER
104
NO
YES
CHANNEL ID ?
105
YES
NO
Null ?
108
YES
NO
Adapt. Field?
110
YES
NO
Table ID?
112
YES
NO
Section Length?
114
YES
NO
Payload ?
116
YES
TYPE = 011
106
TYPE = 010
107
TYPE = 000
109
TYPE = 101
111
TYPE = 110
113
TYPE = 001
115
TYPE = 111
117
SCRAMBLED ?
118
YES
SCR=1
119
NO
SCR=1
120
LAST BYTE ?
121
YES
LTB=1
122
NO
LTB=0
123
OUTPUT QUALIFIED BYTE
124

Fig. 23

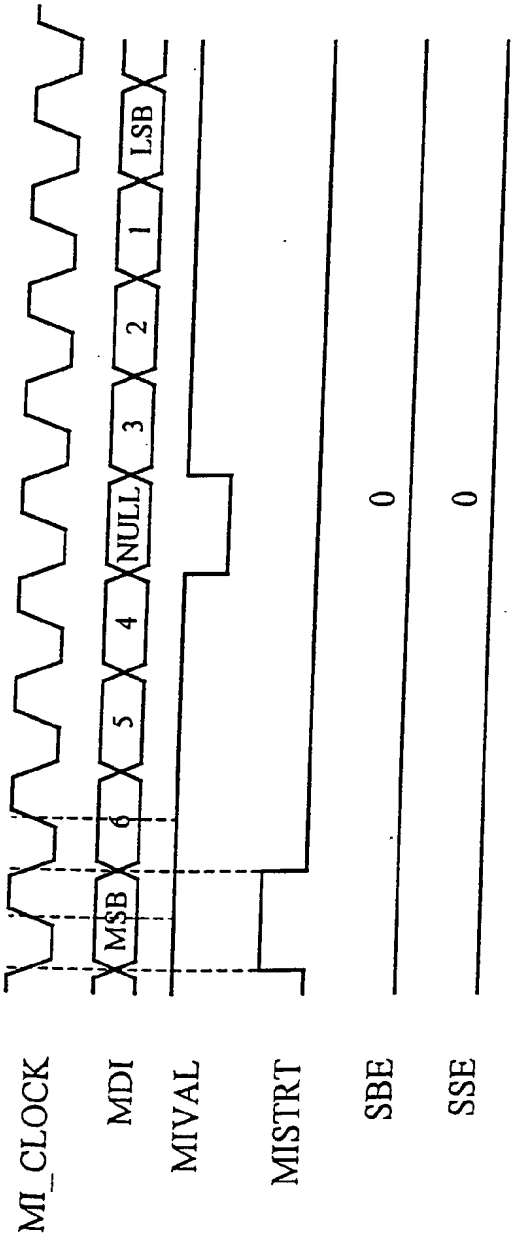


Fig. 24

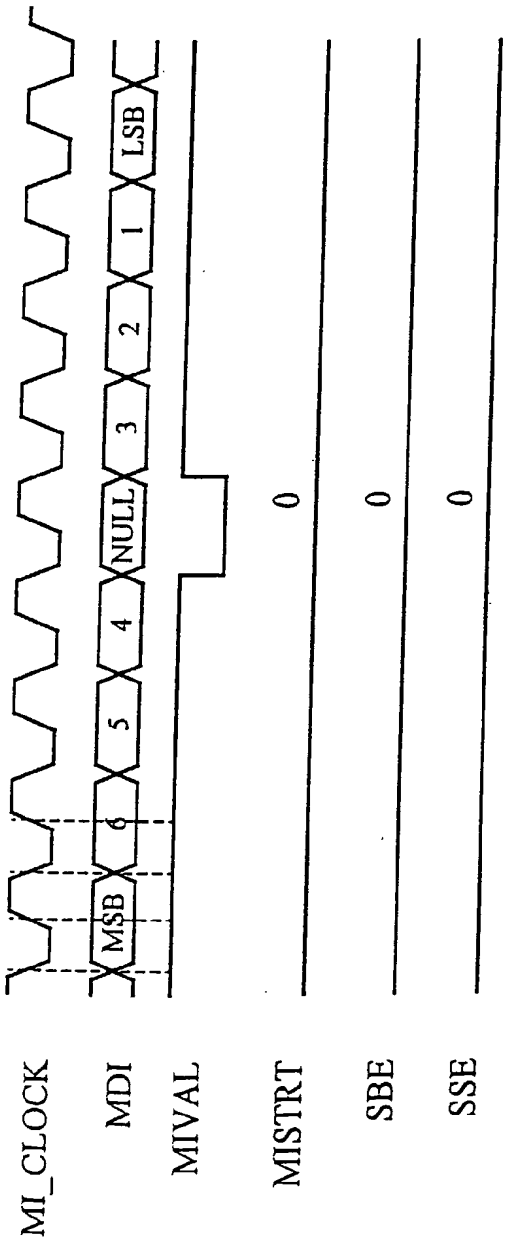


Fig. 25

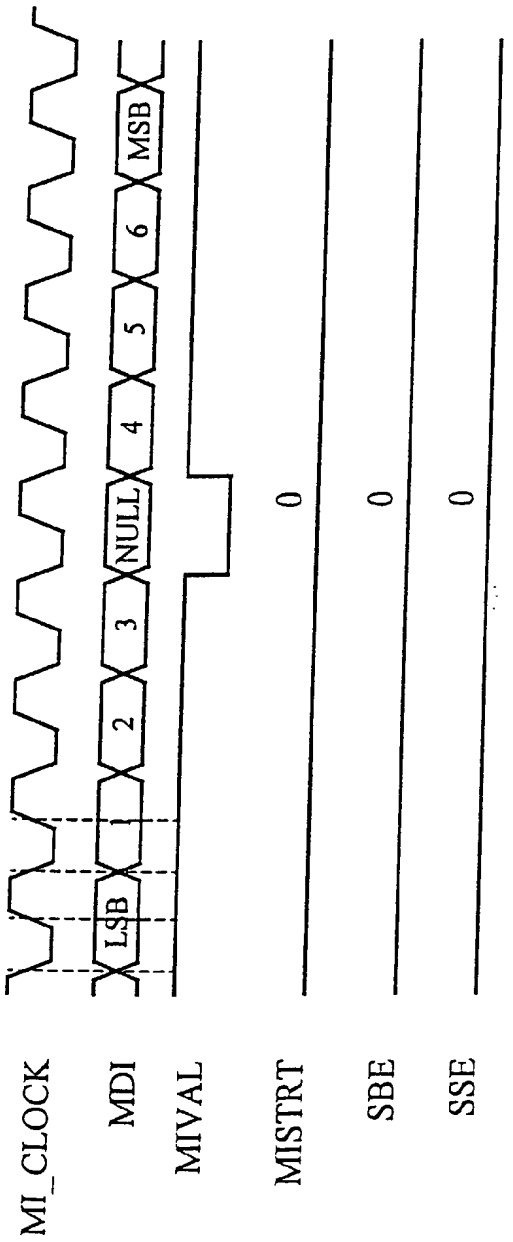


Fig. 26

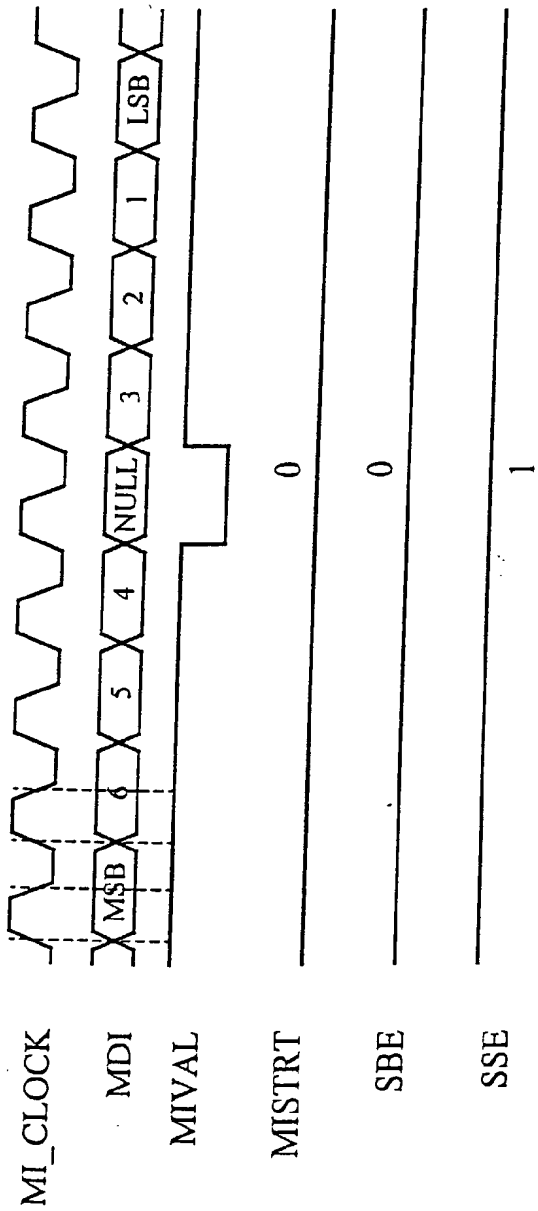


Fig. 27

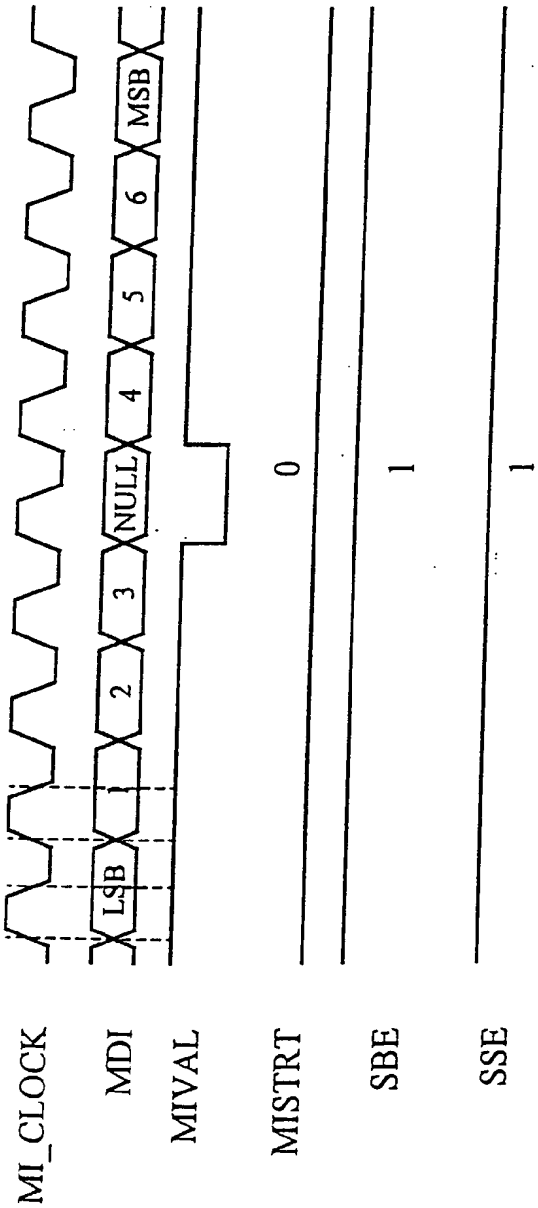


Fig. 28

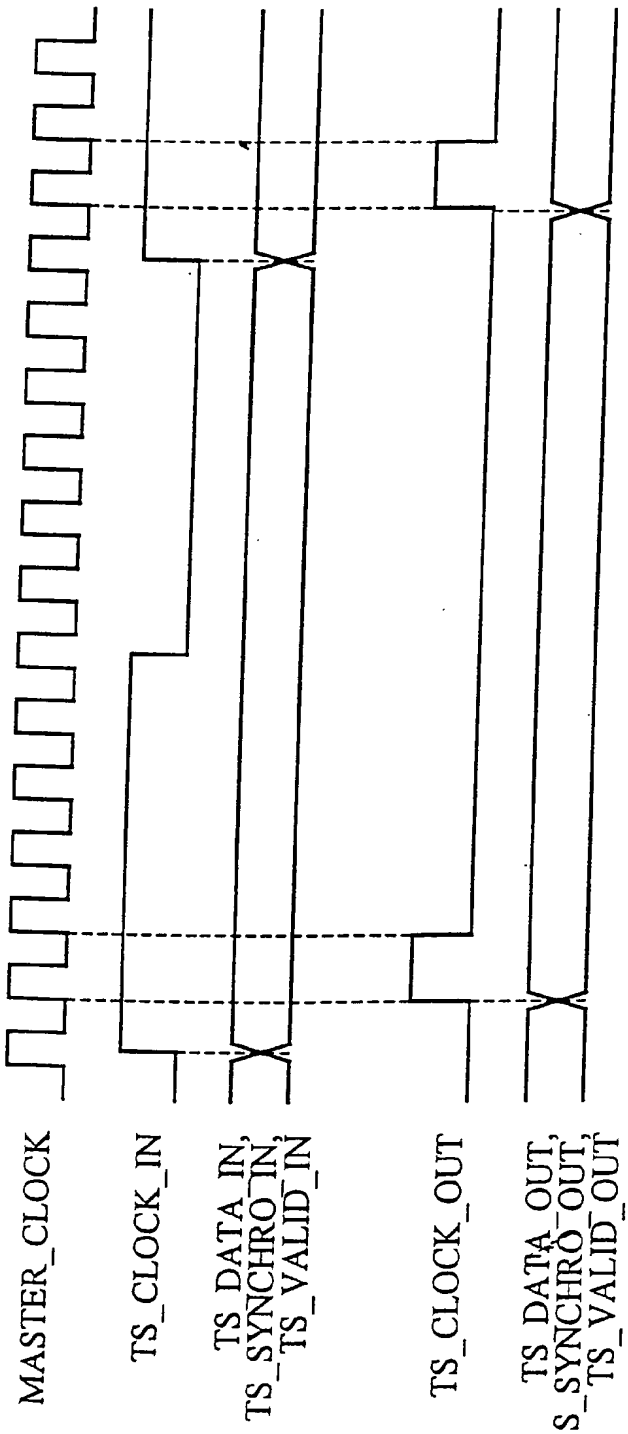

MASTER_CLOCK
TS_CLOCK_IN
TS_DATA_IN,
TS_SYNCHRO_IN,
TS_VALID_IN
TS_CLOCK_OUT
TS_DATA_OUT,
S_SYNCHRO_OUT,
TS_VALID_OUT

Fig. 29

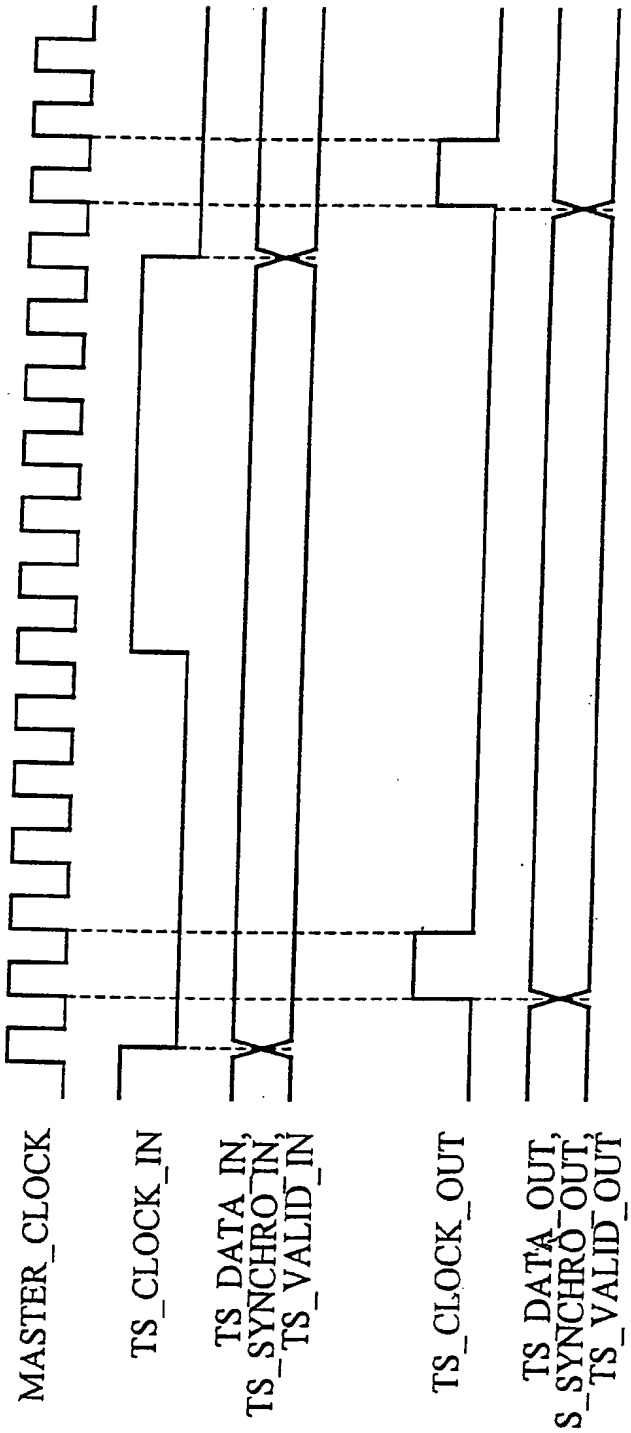

MASTER_CLOCK
TS_CLOCK_IN
TS_DATA_IN,
TS_SYNCHRO_IN,
TS_VALID_IN
TS_CLOCK_OUT
TS_DATA_OUT,
S_SYNCHRO_OUT,
TS_VALID_OUT

Fig. 30

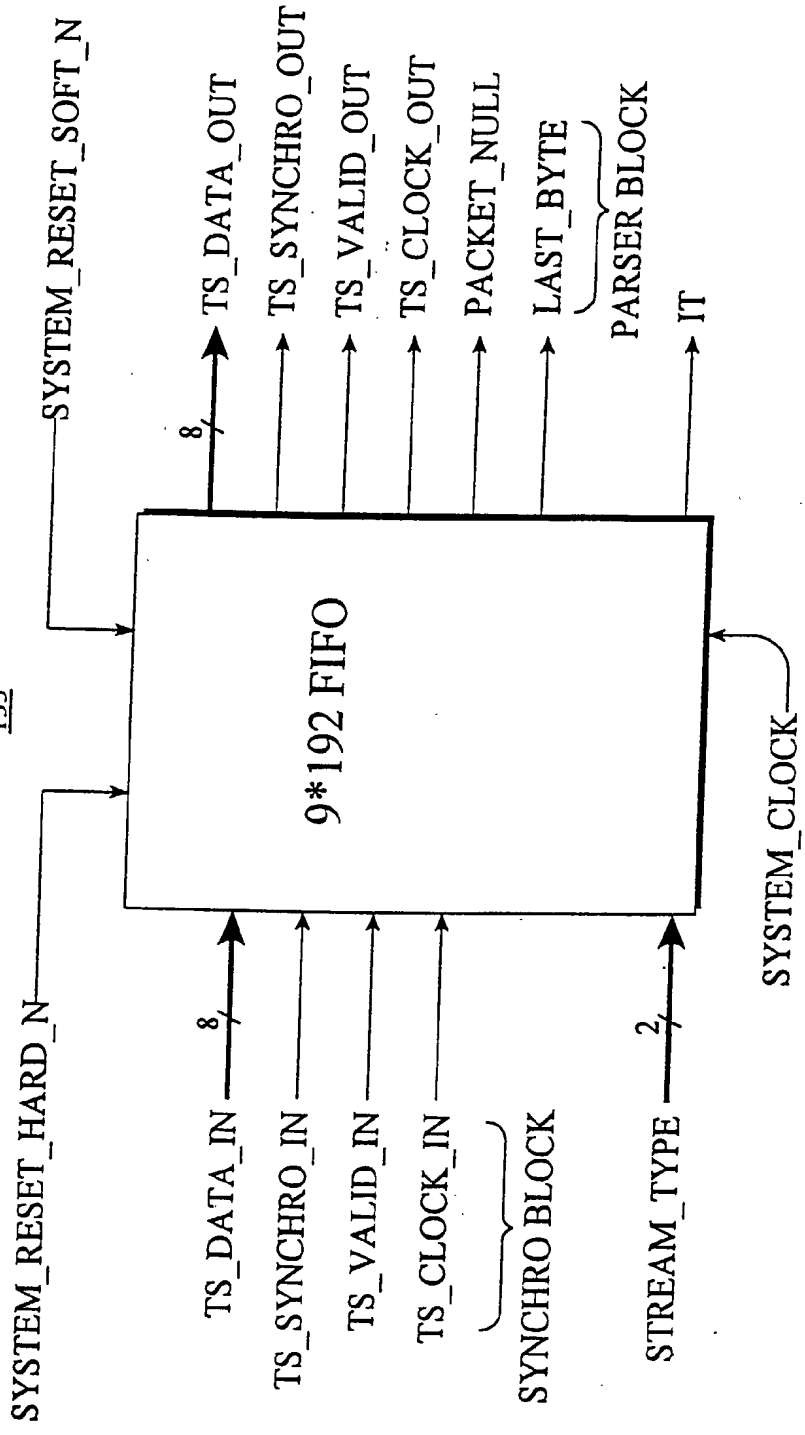

135
9*192 FIFO
SYSTEM_RESET_SOFT_N
SYSTEM_RESET_HARD_N
TS_DATA_OUT
TS_SYNCHRO_OUT
TS_VALID_OUT
TS_CLOCK_OUT
PACKET_NULL
LAST_BYTE
PARSER BLOCK
IT
8
TS_DATA_IN
TS_SYNCHRO_IN
TS_VALID_IN
TS_CLOCK_IN
SYNCHRO BLOCK
STREAM_TYPE
2
SYSTEM_CLOCK

Fig. 31

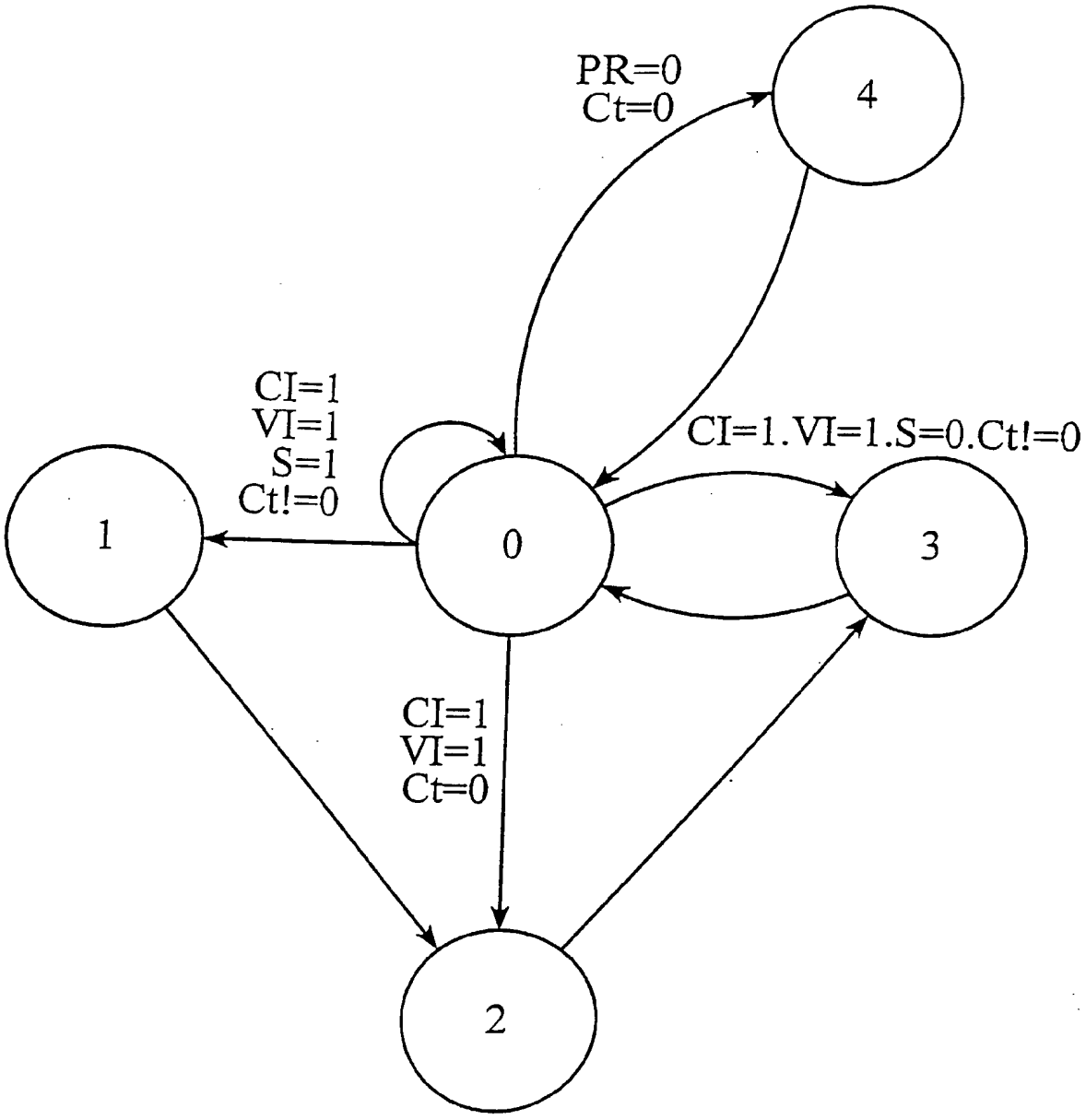


Fig. 32

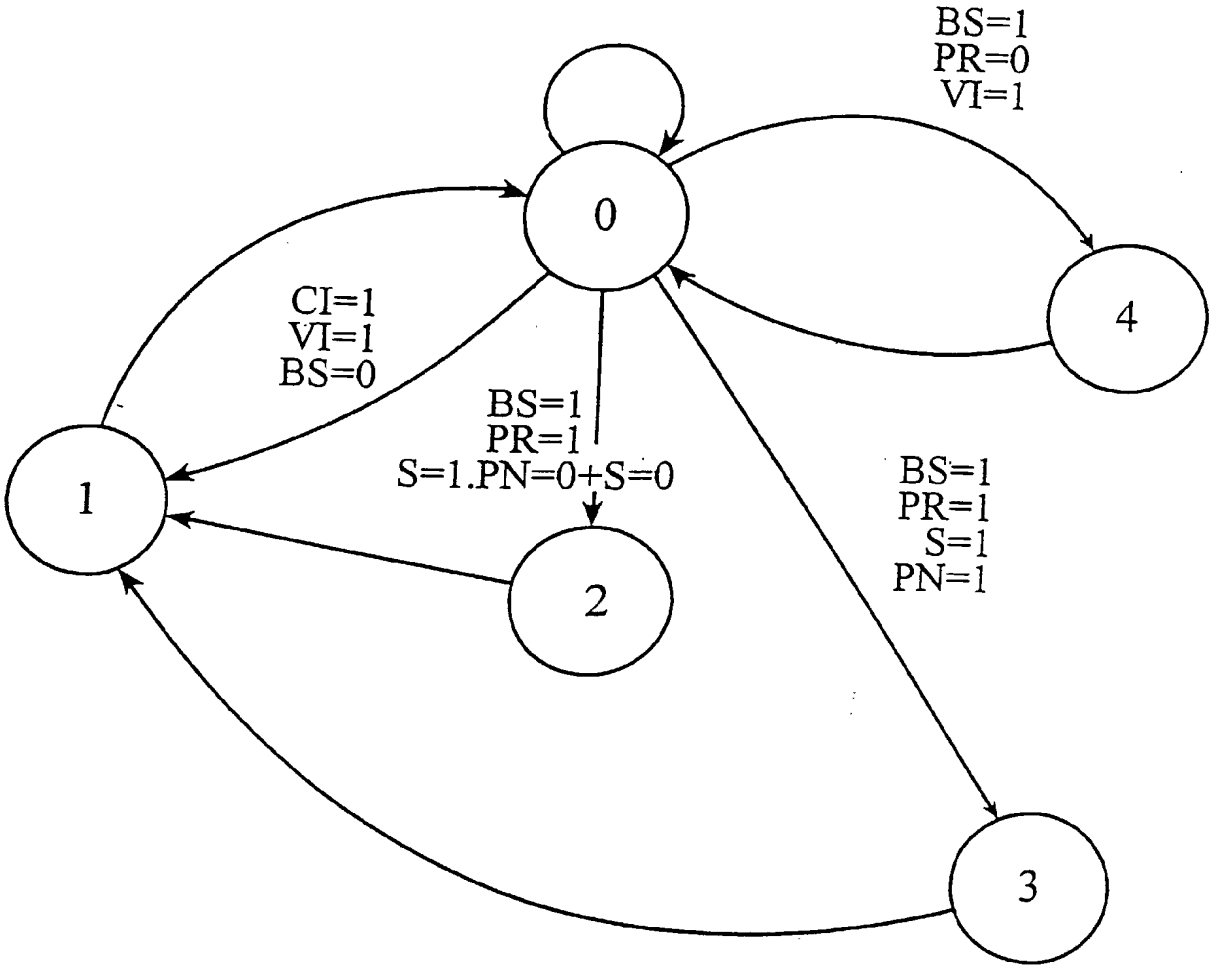


Fig. 32A

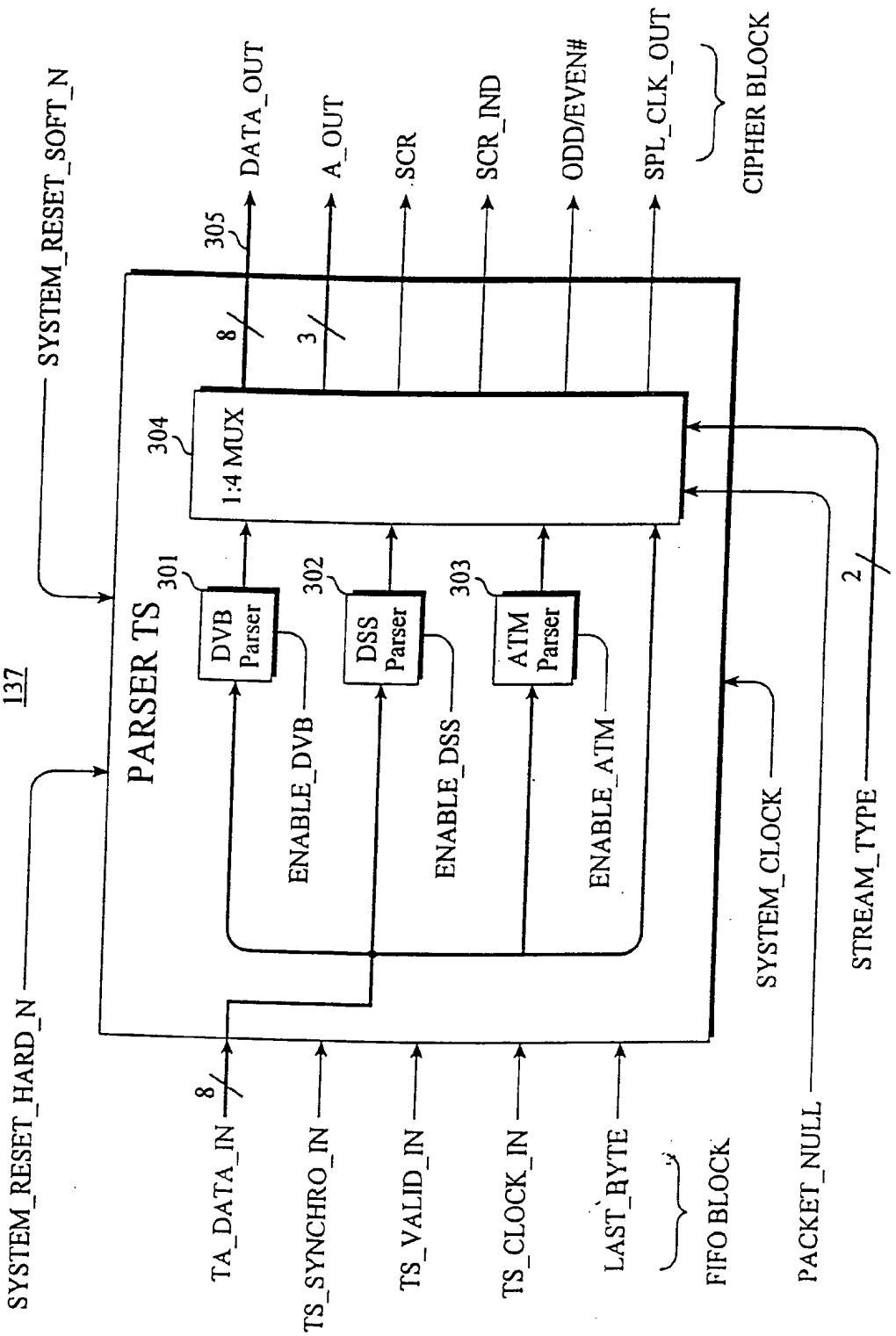

137
PARSER TS
SYSTEM_RESET_HARD_N
SYSTEM_RESET_SOFT_N
TA_DATA_IN
TS_SYNCHRO_IN
TS_VALID_IN
TS_CLOCK_IN
LAST_BYTE
FIFO BLOCK
PACKET_NULL
SYSTEM_CLOCK
STREAM_TYPE
2
8
DVB Parser
DSS Parser
ATM Parser
301
302
303
ENABLE_DVB
ENABLE_DSS
ENABLE_ATM
304
1:4 MUX
305
8
3
DATA_OUT
A_OUT
SCR
SCR_IND
ODD/EVEN#
SPL_CLK_OUT
CIPHER BLOCK

Fig. 33

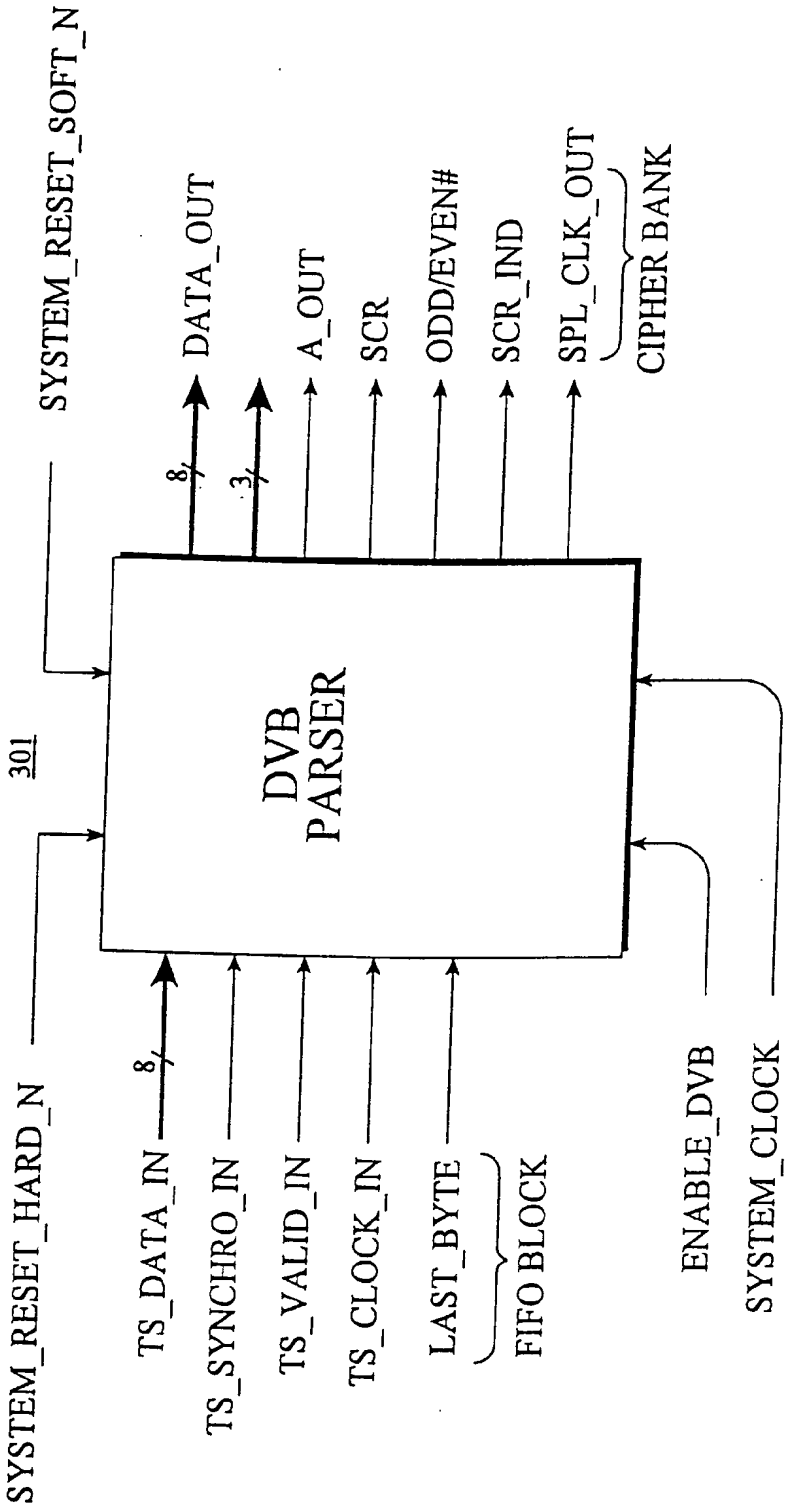

SYSTEM_RESET_SOFT_N
DATA_OUT
A_OUT
SCR
ODD/EVEN#
SCR_IND
SPL_CLK_OUT
CIPHER BANK
8
3
301
DVB
PARSER
SYSTEM_RESET_HARD_N
TS_DATA_IN
TS_SYNCHRO_IN
TS_VALID_IN
TS_CLOCK_IN
LAST_BYTE
FIFO BLOCK
ENABLE_DVB
SYSTEM_CLOCK

Fig. 34

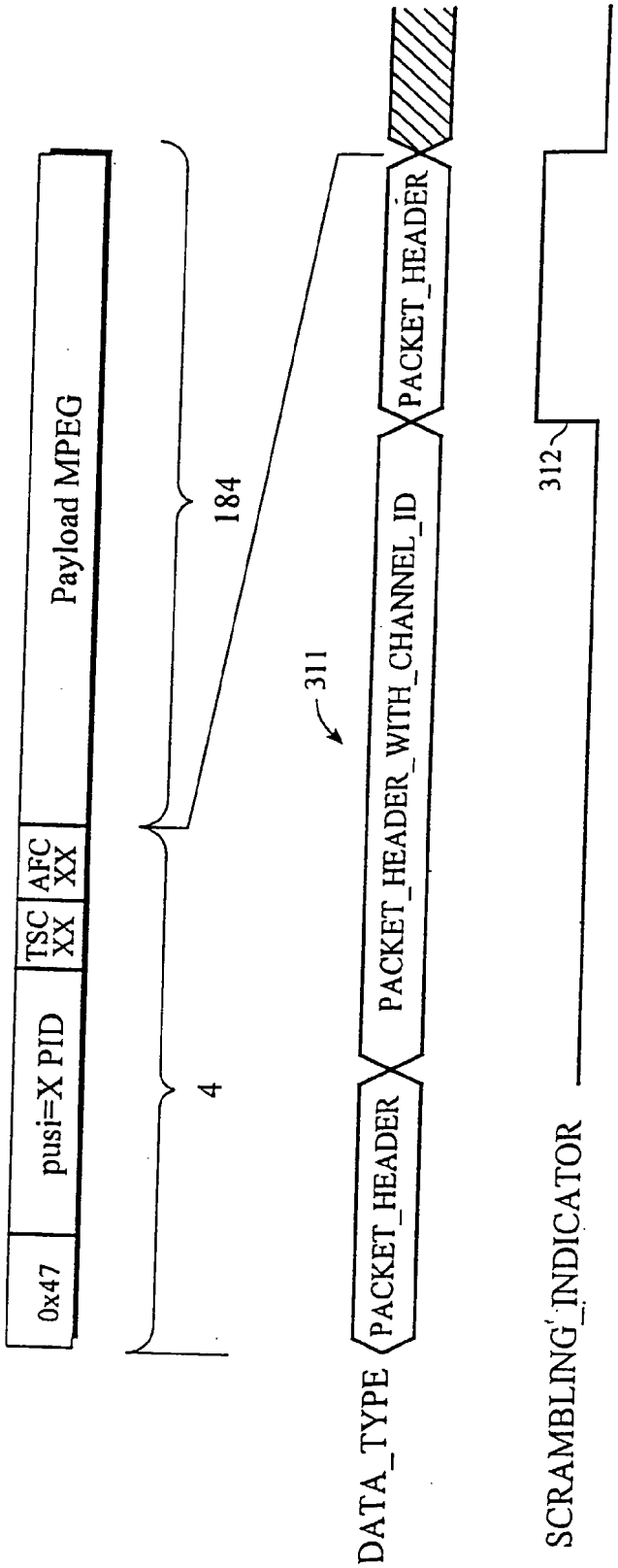

310
0x47
pusi=X PID
TSC XX
AFC XX
Payload MPEG
184
4
311
DATA_TYPE
PACKET_HEADER
PACKET_HEADER_WITH_CHANNEL_ID
PACKET_HEADER
312
SCRAMBLING_INDICATOR

Fig. 35

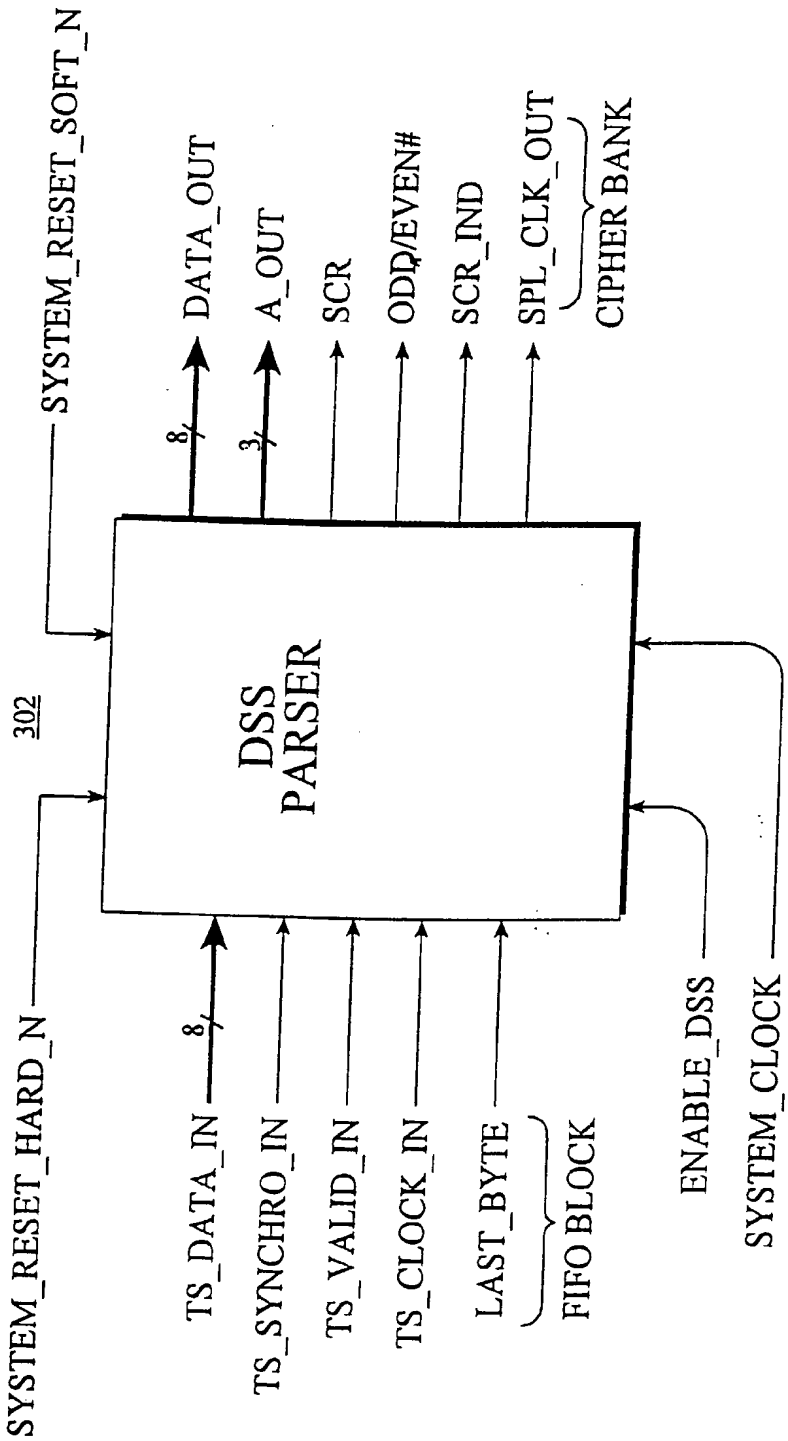

SYSTEM_RESET_SOFT_N
DATA_OUT
A_OUT
SCR
ODD/EVEN#
SCR_IND
SPL_CLK_OUT
CIPHER BANK
8
3
302
DSS
PARSER
SYSTEM_RESET_HARD_N
TS_DATA_IN
TS_SYNCHRO_IN
TS_VALID_IN
TS_CLOCK_IN
LAST_BYTE
FIFO BLOCK
ENABLE_DSS
SYSTEM_CLOCK

Fig. 36

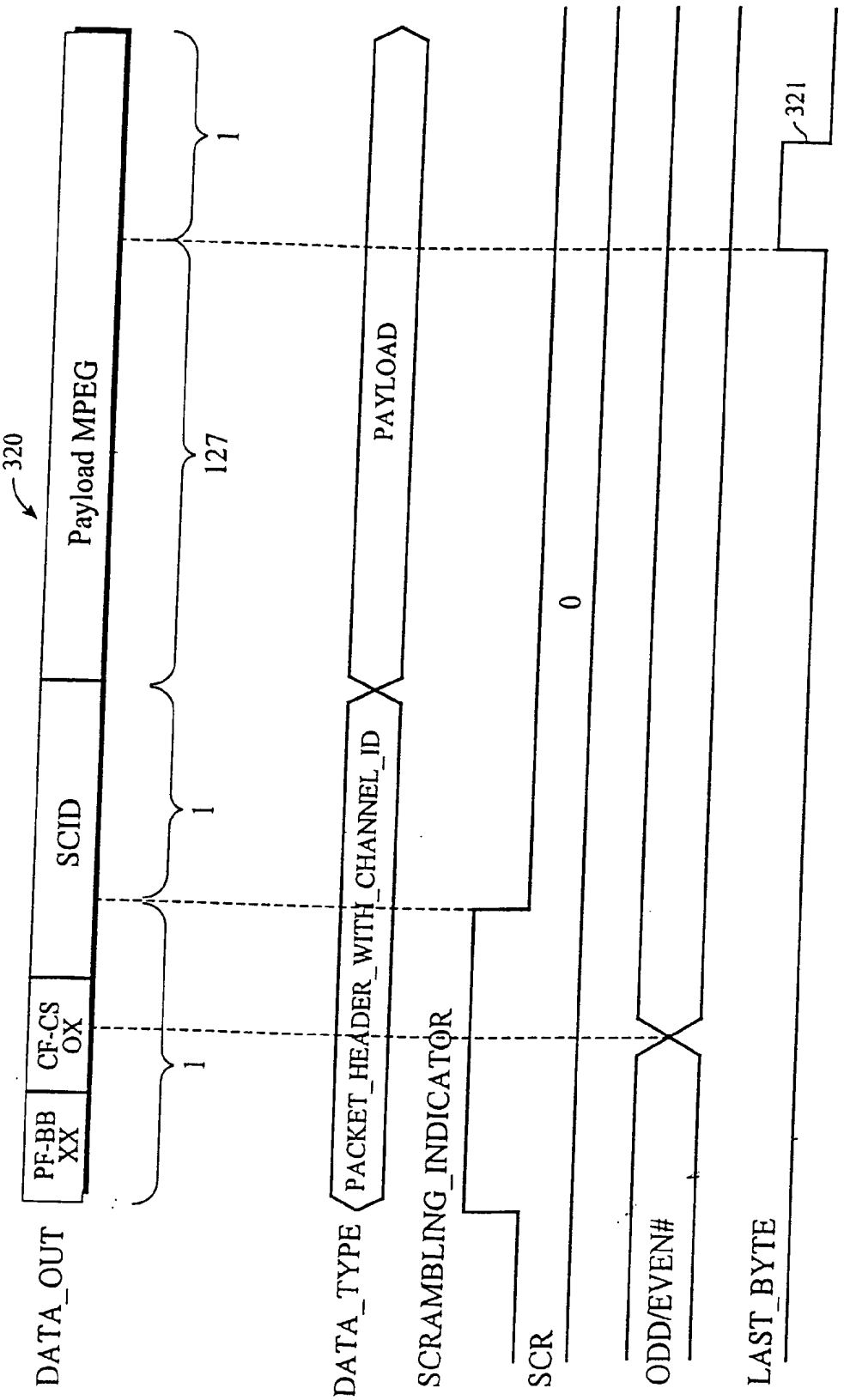

DATA_OUT
PF-BB XX
CF-CS OX
SCID
Payload MPEG
320
1
1
127
1
DATA_TYPE
PACKET_HEADER_WITH_CHANNEL_ID
PAYLOAD
SCRAMBLING_INDICATOR
SCR
0
ODD/EVEN#
LAST_BYTE
321

Fig. 37

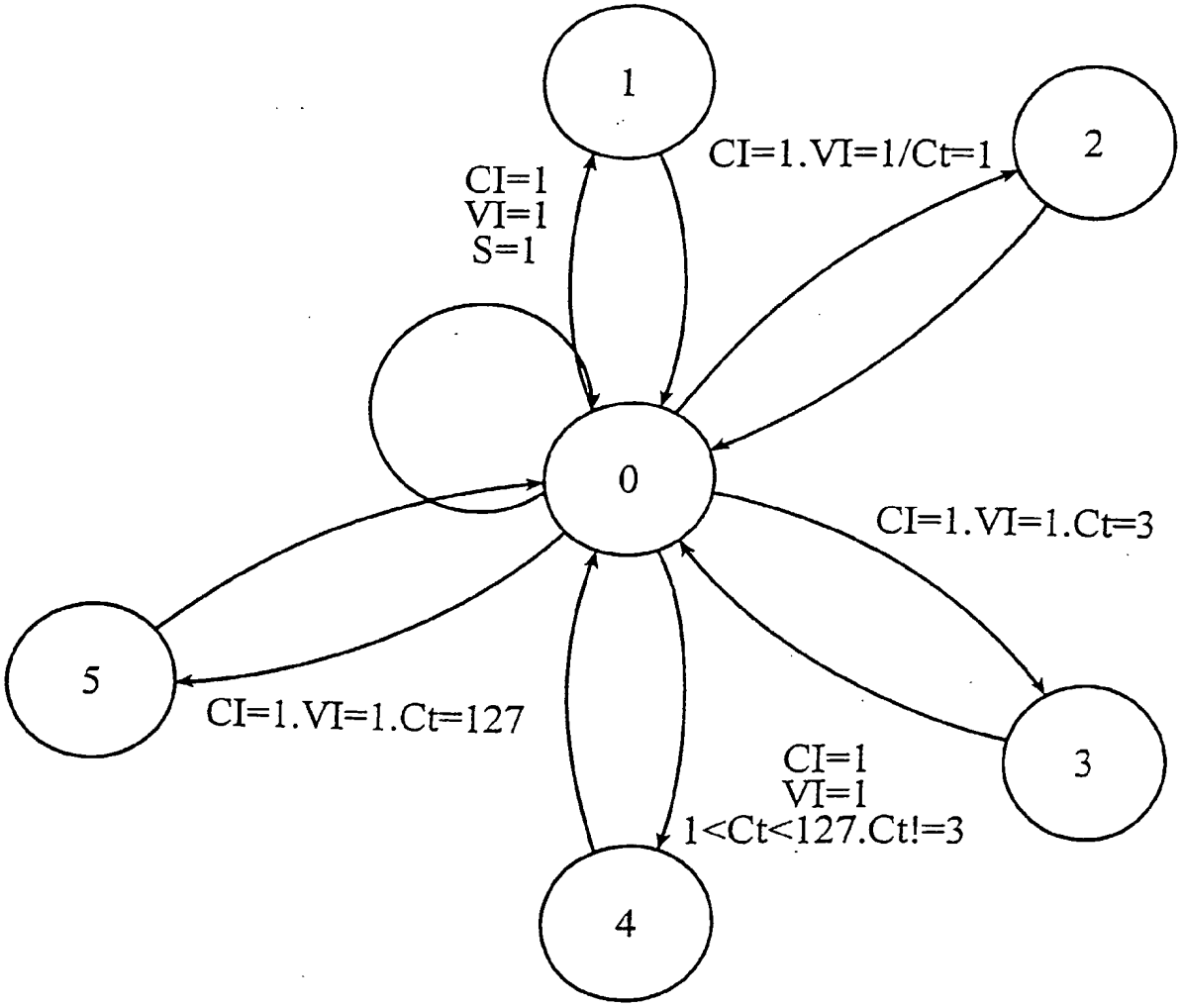

1
2
CI=1
VI=1
S=1
CI=1.VI=1/Ct=1
0
CI=1.VI=1.Ct=3
5
CI=1.VI=1.Ct=127
3
CI=1
VI=1
1<Ct<127.Ct!=3
4

Fig. 38

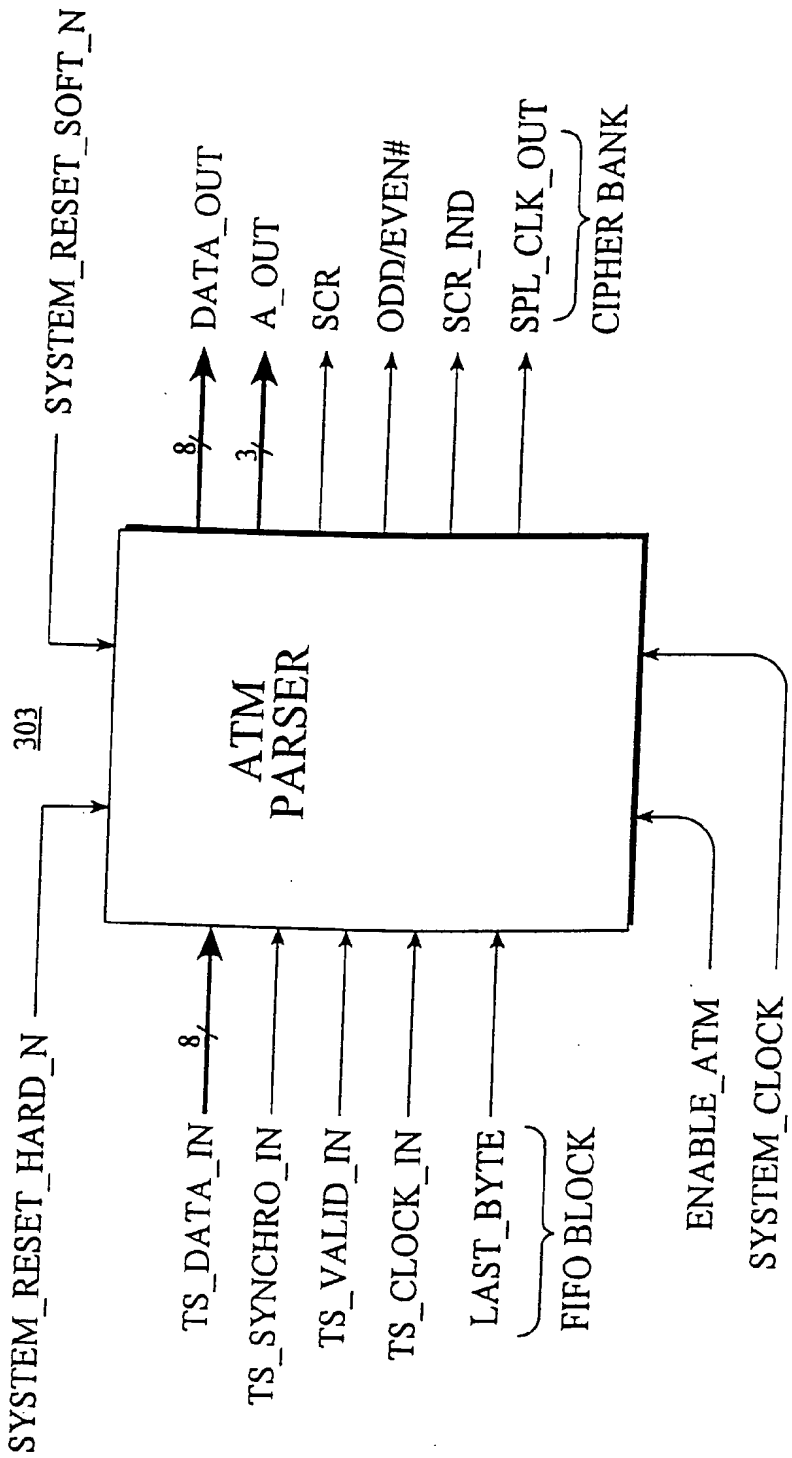

SYSTEM_RESET_SOFT_N
303
ATM
PARSER
SYSTEM_RESET_HARD_N
TS_DATA_IN
8
TS_SYNCHRO_IN
TS_VALID_IN
TS_CLOCK_IN
LAST_BYTE
FIFO BLOCK
ENABLE_ATM
SYSTEM_CLOCK
DATA_OUT
8
A_OUT
3
SCR
ODD/EVEN#
SCR_IND
SPL_CLK_OUT
CIPHER BANK

Fig. 39

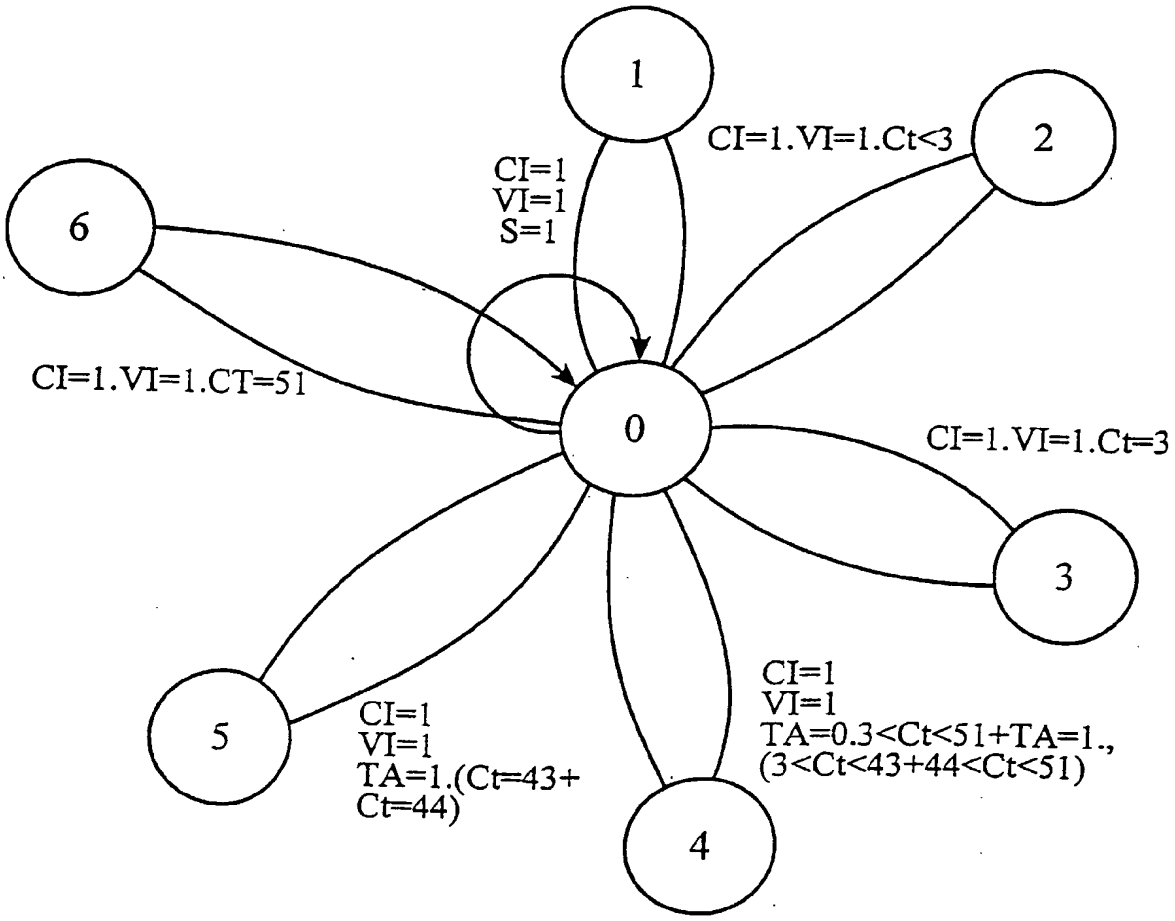

1
2
3
4
5
6
0
CI=1
VI=1
S=1
CI=1.VI=1.Ct<3
CI=1.VI=1.CT=51
CI=1.VI=1.Ct=3
CI=1
VI=1
TA=1.(Ct=43+
Ct=44)
CI=1
VI=1
TA=0.3<Ct<51+TA=1.,
(3<Ct<43+44<Ct<51)

Fig. 40

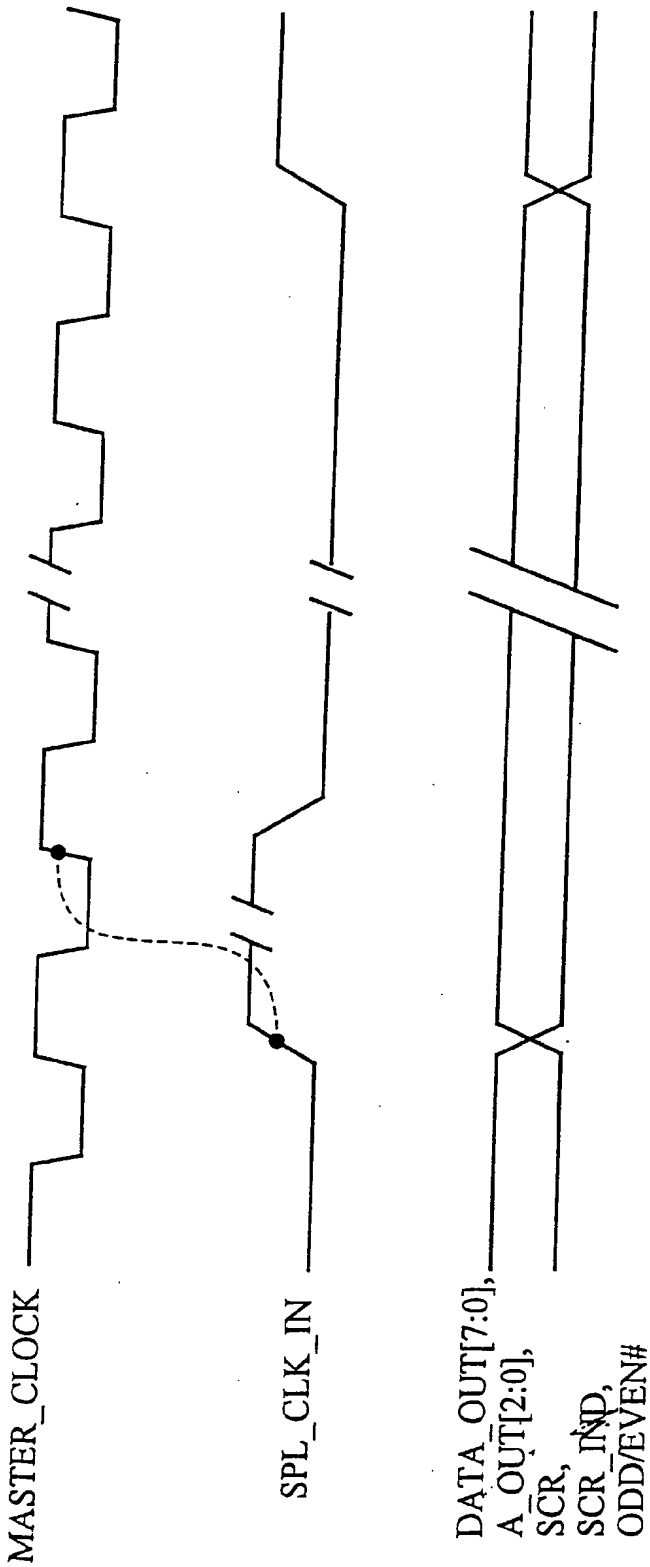

MASTER_CLOCK
SPL_CLK_IN
DATA_OUT[7:0],
A_OUT[2:0],
SCR,
SCR_IND,
ODD/EVEN#

Fig. 41

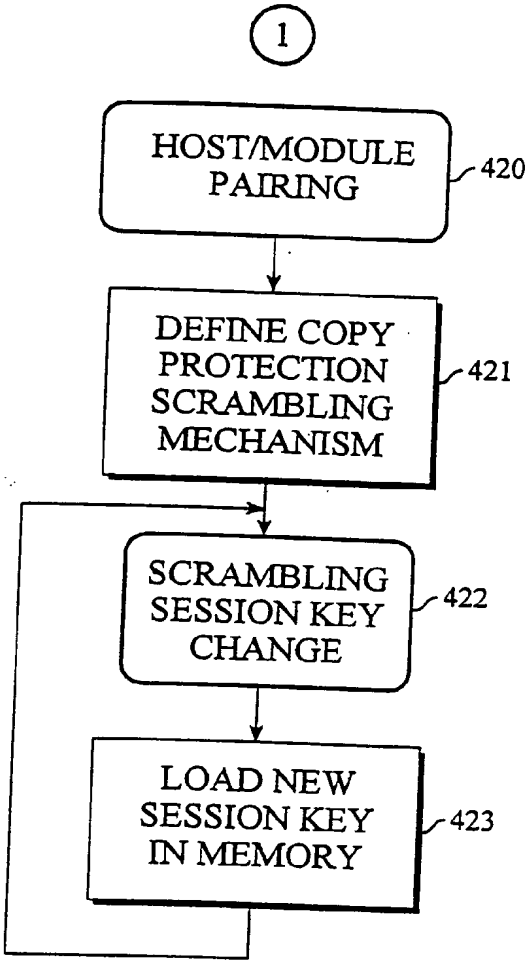

1
419
HOST/MODULE PAIRING
420
DEFINE COPY PROTECTION SCRAMBLING MECHANISM
421
SCRAMBLING SESSION KEY CHANGE
422
LOAD NEW SESSION KEY IN MEMORY
423

Fig. 42

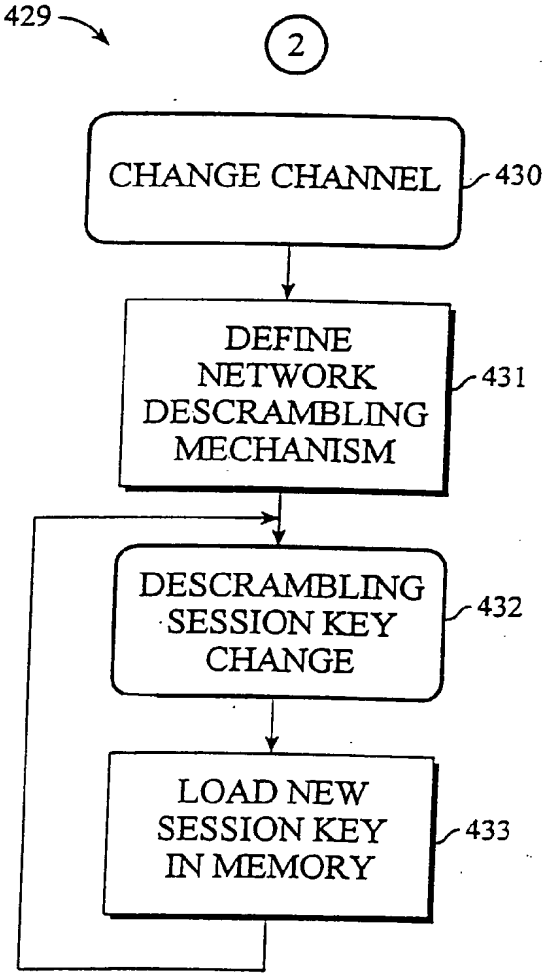

429
2
CHANGE CHANNEL
430
DEFINE NETWORK DESCRAMBLING MECHANISM
431
DESCRAMBLING SESSION KEY CHANGE
432
LOAD NEW SESSION KEY IN MEMORY
433

Fig. 43

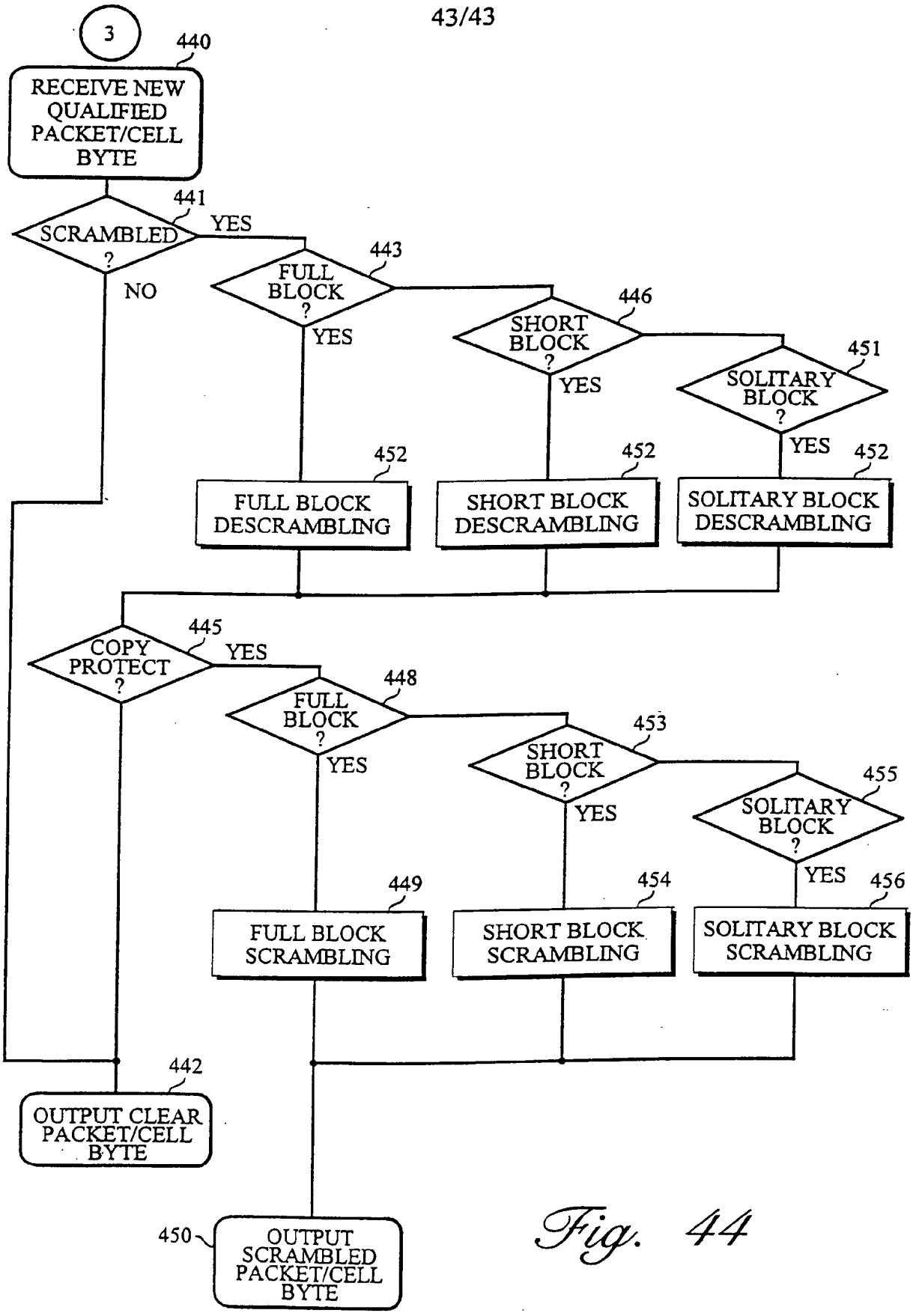

3
440
RECEIVE NEW QUALIFIED PACKET/CELL BYTE
441
SCRAMBLED ?
YES
NO
443
FULL BLOCK ?
YES
446
SHORT BLOCK ?
YES
451
SOLITARY BLOCK ?
YES
452
FULL BLOCK DESCRAMBLING
452
SHORT BLOCK DESCRAMBLING
452
SOLITARY BLOCK DESCRAMBLING
445
COPY PROTECT ?
YES
448
FULL BLOCK ?
YES
453
SHORT BLOCK ?
YES
455
SOLITARY BLOCK ?
YES
449
FULL BLOCK SCRAMBLING
454
SHORT BLOCK SCRAMBLING
456
SOLITARY BLOCK SCRAMBLING
442
OUTPUT CLEAR PACKET/CELL BYTE
450
OUTPUT SCRAMBLED PACKET/CELL BYTE

Fig. 44

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/EP 00/11485

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N5/913 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 763 936 A (LG ELECTRONICS INC) 19 March 1997 (1997-03-19) page 4, column 6, line 31 -page 15, column 28, line 21 figures 3-26 ---	1-4,6-8, 10-12, 72-81 23-71, 82-89
A	EP 0 691 787 A (SONY CORP) 10 January 1996 (1996-01-10) page 3, column 3, line 3 -page 11, column 20, line 1 figures 1-7 --- -/--	1-89

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 April 2001	25/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van der Zaal, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter I Application No
PCT/EP 00/11485

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) page 1, column 1, line 23 - line 39 page 5, column 7, line 48 -page 7, column 12, line 38 figures 1-5	1-89

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr Application No
PCT/EP 00/11485

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0763936 A	19-03-1997	KR 166923 B	20-03-1999
		CN 1150738 A	28-05-1997
		JP 9093561 A	04-04-1997
		US 5799081 A	25-08-1998
EP 0691787 A	10-01-1996	CN 1115150 A	17-01-1996
		EP 0975165 A	26-01-2000
		JP 8077706 A	22-03-1996
		US 5796828 A	18-08-1998
EP 0858184 A	12-08-1998	IL 120174 A	28-10-1999
		US 6178242 B	23-01-2001
		GB 2322030 A,B	12-08-1998

DERWENT-ACC-NO: 2001-564999

DERWENT-WEEK: 200163

TITLE: Method of real time adaptive descrambling and scrambling for digital television by encrypting received data if copy protection indicia are included

INVENTOR: CHATAIGNIER A; GENEVOIS C ; VANTALON L

PATENT-ASSIGNEE: SCM MICROSYSTEMS GMBH[SCMMN]

PRIORITY-DATA: 1999US-444490 (November 19, 1999)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
WO 0137562 A1	May 25, 2001	EN

DESIGNATED-STATES: JP SG AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
WO2001037562A1	N/A	2000WO-EP11485	November 17, 2000

INT-CL-CURRENT:

TYPE	IPC DATE
CIPS	H04N5/913 20060101
CIPS	H04N7/16 20060101

CIPS H04N9/804 20060101

ABSTRACTED-PUB-NO: WO 0137562 A1

BASIC-ABSTRACT:

NOVELTY - Method consists in receiving data in data units, determining its encryption state, and providing a clear output if it is unencrypted. If it is encrypted the data unit size is found for decryption, it is determined whether the decrypted data includes copy protection indicia, and if it does, encryption is performed and the data is output. A selected host is paired with a selected module, the desired scrambling format is selected, and the selected session key is loaded into a memory. Broadcast and burst signals are processed for scrambling.

DESCRIPTION - The scrambling formats are DVB, DES-ECB, DES-CBC, DES-OFB, MULTI2, 3DES-ECB, 3DES-CBC, 3DES-OFB, DVB being digital video broadcasting, DES is data encryption standard, ECB is electronic code book, CBC is chain block cipher, OFB is output feedback block. There are INDEPENDENT CLAIMS for (1) a copy protect scrambler, (2) a method of multiple scrambling, (3) a method of signal processing, (4) a method of enabling a conditional access module to handle transport stream formats, (5) a method of handling transport stream formats, (6) a system for receiving transport stream formats, (7) a receiver and security mechanism system, (8) a set-top system, (9) a digital signal receiver, (10) a method of trans-scrambling bytes of received information, (11) a method of processing bytes of information.

USE - Method relates to multiple data streams used in the transfer of data in different encryption formats in digital television.

ADVANTAGE - Method is for use with a universal set-top box and grants conditional access to transmitted program material to protect against unauthorized use of the material.

DESCRIPTION OF DRAWING(S) - The figure shows a digital TV receiving system with a security mechanism for preventing unauthorized display of

transmitted images.

CHOSEN-DRAWING: Dwg.1/44

TITLE-TERMS: METHOD REAL TIME ADAPT SCRAMBLE DIGITAL TELEVISION RECEIVE DATA COPY PROTECT INDICIA

DERWENT-CLASS: W02 W04

EPI-CODES: W02-F05A; W04-F01L;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: 2001-420674